

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 9 月 29 日 (29.09.2005)

PCT

(10) 国際公開番号
WO 2005/091150 A1

- (51) 国際特許分類: G06F 12/14, G11B 20/10, H04N 5/91
- (21) 国際出願番号: PCT/JP2005/005253
- (22) 国際出願日: 2005 年 3 月 23 日 (23.03.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2004-085364 2004 年 3 月 23 日 (23.03.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1006 番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 井藤 好克 (ITO,

Yoshikatsu). 宮崎 雅也 (MIYAZAKI, Masaya). 大森 基司 (OHMORI, Motoji). 原田 俊治 (HARADA, Shunji). 横田 薫 (YOKOTA, Kaoru). 中野 稔久 (NAKANO, Toshihisa). 高橋 潤 (TAKAHASHI, Jun).

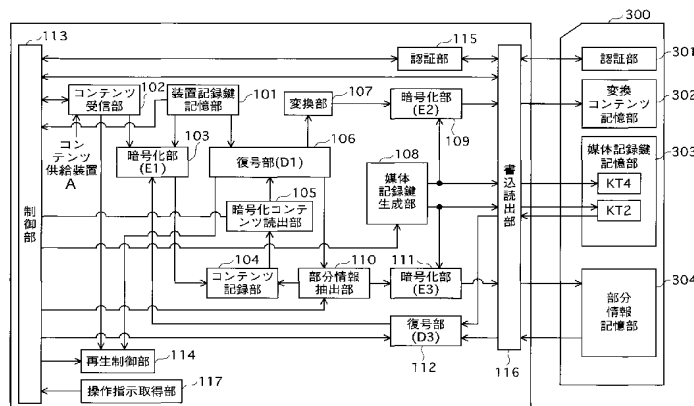
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目 2 番 1 号淀川 5 番館 6 F Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: CONTENT MOVEMENT DEVICE, CONTENT MOVEMENT METHOD, COMPUTER PROGRAM, RECORDING MEDIUM, AND CONTENT MOVEMENT SYSTEM

(54) 発明の名称: コンテンツ移動装置、コンテンツ移動方法、コンピュータプログラム、記録媒体及びコンテンツ移動システム



115... AUTHENTICATION UNIT
102... CONTENT RECEPTION UNIT
101... DEVICE RECORDING KEY STORAGE UNIT
107... CONVERSION UNIT
109... ENCRYPTION UNIT (E2)
113... CONTROL UNIT
A... CONTENT SUPPLY DEVICE
103... ENCRYPTION UNIT (E1)
106... DECRYPTION UNIT (D1)
108... MEDIUM RECORDING KEY GENERATION UNIT
105... ENCRYPTED CONTENT READ OUT UNIT

104... CONTENT RECORDING UNIT
110... PARTIAL INFORMATION EXTRACTION UNIT
111... ENCRYPTION UNIT (E3)
112... DECRYPTION UNIT (D3)
114... REPRODUCTION CONTROL UNIT
117... OPERATION INSTRUCTION ACQUISITION UNIT
116... WRITE-IN/READ-OUT UNIT
301... AUTHENTICATION UNIT
302... CONVERTED CONTENT STORAGE UNIT
303... MEDIUM RECORDING KEY STORAGE UNIT
304... PARTIAL INFORMATION STORAGE UNIT

(57) Abstract: There is provided a user-friendly content movement device capable of preventing unauthorized copying of a content and enabling a user to use a content before subjected to irreversible conversion when the content which has been irreversibly converted and moved to a recording medium is returned to the move source. A partial information extraction unit (110) extracts from a content stored in a content

[続葉有]



WO 2005/091150 A1



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

storage unit (104), partial data required for reproducing the content. A write/read unit (116) performs write into a partial information storage unit (304) and overwrites the part corresponding to the partial data of the content by another data. A conversion unit (107) transcodes the content and writes it in the recording medium.

(57) 要約: 本発明は、コンテンツの不正コピーを防止し、かつ、不可逆変換した後に記録媒体にムーブされたコンテンツをムーブ元に戻した場合に、不可逆変換前のコンテンツを使用することができる、ユーザにとって利便性の高いコンテンツ移動装置を提供することを目的とする。コンテンツ記録部104に記憶されたコンテンツから、部分情報抽出部110が当該コンテンツの再生に必要な部分データを抽出し、書込読出部116が部分情報記憶部304に書き込むと共に前記コンテンツの部分データ相当部分を他のデータで上書きすると共に、変換部107が前記コンテンツをトランスコードして、前記記録媒体に書き込む。

明 細 書

コンテンツ移動装置、コンテンツ移動方法、コンピュータプログラム、記録媒体及びコンテンツ移動システム

技術分野

- [0001] 本発明は、コンテンツ移動装置及び記録媒体を含むコンテンツ移動システムに関し、特に、コンテンツの不正利用を防止し、かつユーザの利便性を向上させる技術に関する。

背景技術

- [0002] 近年、BSデジタル放送や地上デジタル放送等により、映画等のデジタルコンテンツ(以下、コンテンツという。)が広く配信されている。

前記コンテンツには、複製が容易であり、複製に伴う劣化がないという特徴があるので、著作権保護を目的とした、コンテンツの複製可否の制御、複製の世代管理を行うためのコピー制御情報(CCI: Copy Control Information)が付加されている。

- [0003] 例えば、CCIに、コンテンツのコピーが1回だけ許可されていることを表す「Copy One Generation」が設定されている場合、当該コンテンツをコピーすると、コピーによって新たに得られたコンテンツには、コピー制御情報としてコピー不可を示す「Copy No More」が設定される。

CCIに「Copy No More」が設定されている場合、当該コンテンツを他の記録媒体又は装置へコピーすることは出来ないが、著作権を保護しつつ移動することは可能である(特許文献1参照)。

- [0004] これは、デジタルテレビに内蔵されているHDD(Hard Disk Drive)に記録されているコンテンツをSDカードに移動させるような場合が該当するが、コンテンツを移動した後、前記HDDに記録されているコンテンツを消去するなどして移動先のSDカード内のコンテンツ以外のコンテンツを利用できない状態にしなければならない。

また、移動元のコンテンツが高画質でありサイズが大きく、移動先のSDカードの記録容量が前記コンテンツのサイズに比べ小さい場合には、移動前に前記コンテンツを低画質に変換してサイズを小さくしてから移動を行うことが、よく行われている。

特許文献1:特開2003-228522号公報

発明の開示

発明が解決しようとする課題

- [0005] しかしながら、一旦、コンテンツを記録容量の小さい移動(ムーブ)先へ移動してしまふと、記録容量の小さい前記ムーブ先から、再び記録容量の大きなムーブ元の前記HDDへムーブし直しても、低画質のコンテンツしか再生できなくなり、ユーザにとっては、不便である。

上記の問題に鑑み、本発明は、コンテンツの不正コピーを防止し、かつ、不可逆変換を行った後にムーブしたコンテンツをムーブ元に戻した場合に、ムーブ元において変換前のコンテンツが復元出来る、ユーザにとって利便性の高いコンテンツ移動装置、コンテンツ移動方法、コンピュータプログラム、記録媒体及びコンテンツ移動システムを提供することを目的とする。

課題を解決するための手段

- [0006] 上記課題を解決するために、本発明は、記憶しているコンテンツを可搬型の記録媒体に移動するコンテンツ移動装置であって、コンテンツを記憶している記憶手段と、前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成手段と、前記コンテンツの一部である部分データを抽出する抽出手段と、前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換手段と、生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込手段とを備える。

発明の効果

- [0007] 本発明のコンテンツ移動装置は、前述の構成を備えることにより、前記記憶手段に記憶されたコンテンツを再生できないよう無効化し、前記記録媒体に記録された変換コンテンツのみ再生可能として著作権を保護することができる。

また、前記部分データを、前記記憶手段に記憶されているコンテンツの前記無効化された部分に書き戻し、前記記録媒体に記録された変換コンテンツを消去すれば、著作権を保護しつつ、前記コンテンツ移動装置において、記録媒体に移動する前の

コンテンツを復元することができる。

- [0008] また、前記抽出手段は、前記コンテンツの所定位置から、所定長の前記部分データを抽出してもよい。

この構成によれば、コンテンツにおける所定位置から所定長のデータを無効化できるので、コンテンツを再生不可能にすることができる。

例えば、所定位置から所定長のデータ部分には、再生に不可欠な制御データが入っている場合、コンテンツの再生は不可能となる。

- [0009] また、前記コンテンツは、少なくともフレーム内符号化された圧縮フレーム画像を含み、前記抽出手段は、前記部分データとして、フレーム内符号化された前記圧縮フレーム画像の一部又は全部を抽出してもよい。

この構成によれば、フレーム内符号化された圧縮フレーム画像の一部又は全部を抽出するので、コンテンツの完全な再生を不可能にして、確実に著作権を保護することができる。

- [0010] また、フレーム間符号化された圧縮フレーム画像も含む場合には、フレーム内符号化された圧縮フレーム画像を再生不可能にすることにより、フレーム間符号化された圧縮フレーム画像も一緒に再生不可能にすることができる。

また、前記コンテンツは、複数の固定長のブロックデータから成り、前記抽出手段は、複数のブロックデータから1のブロックデータを抽出し、抽出したブロックデータ内にフレーム内符号化された前記圧縮フレーム画像の一部が含まれるか否かを判断し、含まれる場合に、抽出したブロックデータを前記部分データとして出力し、前記置換手段は、前記コンテンツにおいて、抽出された前記ブロックデータに相当する部分を他のデータにより置き換えてもよい。

- [0011] この構成によれば、フレーム内符号化された圧縮フレーム画像に係るブロックデータを確実に無効化することができる。

また、前記コンテンツを構成する各ブロックデータは、デジタル著作物が前記固定長毎に暗号化されて生成されたものであり、前記抽出手段は、抽出した前記ブロックデータを復号して復号ブロックデータを生成する復号部と、生成された復号ブロックデータ内にフレーム内符号化された前記圧縮フレーム画像の一部が含まれるか否か

を判断し、含まれる場合に、抽出されたブロックデータを前記部分データとして出力する判断部とを含み、前記置換手段は、前記コンテンツにおいて、フレーム内符号化された前記圧縮フレーム画像の一部が含まれると判断された前記復号ブロックデータに相当する部分を他のデータにより置き換えてもよい。

[0012] この構成によれば、暗号化されたデジタル著作物において、フレーム内符号化された圧縮フレーム画像に係るブロックデータを確実に無効化することができる。

また、前記書込手段は、さらに、前記部分データの前記記録媒体への書き込みに代えて、前記記録媒体の媒体鍵を用いて、フレーム内符号化された前記圧縮フレーム画像の一部が含まれると判断された前記復号ブロックデータを暗号化し、前記暗号化した復号ブロックデータを前記記録媒体に書き込んでよい。

[0013] この構成によれば、復号ブロックデータを暗号化して記録媒体に書き込むので、著作権の保護をより確実に行うことができる。

また、前記書込手段は、前記媒体鍵を保持している鍵保持部と、前記媒体鍵を用いて、前記復号ブロックデータを暗号化する暗号化部と、前記暗号化された復号ブロックデータと、前記媒体鍵とを前記記録媒体に書き込む書込部と、前記鍵保持部に保持されている媒体鍵を消去する鍵消去部とを含んでもよい。

[0014] この構成によれば、抽出された前記復号ブロックデータと、前記コンテンツから抽出された後のデータとのそれぞれの暗号化に用いる鍵を分けて、コンテンツの不正利用をより困難にすることができる。

また、前記抽出手段は、さらに、抽出した前記部分データの前記コンテンツにおける位置を出力し、前記書込手段は、さらに、前記部分データの位置を前記記録媒体に書き込んでよい。

[0015] この構成によれば、前記記録媒体から、前記コンテンツにおける部分データの位置を書き込んでおくので、前記コンテンツを復元する場合に、前記コンテンツにおける前記位置に前記部分データを書き込むことで無効化された前記コンテンツを容易に復元することができる。

また、前記記録媒体に記録されている変換コンテンツを当該コンテンツ移動装置に移動する前記コンテンツ移動装置において、前記記録媒体は、前記変換コンテンツ

と前記部分データとを記録しており、前記記憶手段に記憶されている前記コンテンツにおいて、前記部分データに相当する部分は、他のデータにより置き換えられており、前記コンテンツ移動装置は、さらに、前記変換コンテンツ及び前記部分データが記録されている前記記録媒体から、前記部分データを読み出す読出手段と、前記記憶手段に記憶されている前記コンテンツにおいて、前記他のデータにより置き換えられた部分を、読み出された前記部分データにより置き換える再置換手段と、前記記録媒体から、前記部分データと前記変換コンテンツとを消去する消去手段とを備えてもよい。

- [0016] この構成によれば、前記部分データを、前記記憶手段に記憶されているコンテンツの前記無効化された部分に書き戻してコンテンツを復元し、前記記録媒体に記録された変換コンテンツを消去するので、著作権を確実に保護しつつ、コンテンツ移動装置において、記録媒体に移動する前のコンテンツを復元することができる。

また、前記記憶手段に記憶されている前記コンテンツの所定位置から所定長の部分が、他のデータにより置き換えられており、前記再置換手段は、前記コンテンツの所定位置から所定長の部分を、読み出された前記部分データにより置き換えてもよい。

- [0017] この構成によれば、前記コンテンツの前記所定位置に所定長の前記部分データを書き込むことで無効化された前記コンテンツを容易に復元することができる。

また、前記コンテンツは、複数の固定長のブロックデータから成り、前記記憶手段に記憶されている前記コンテンツの所定位置から所定長の部分に相当するブロックデータが、他のデータにより置き換えられており、前記部分データは、前記複数のブロックデータのうち1のブロックデータであり、前記再置換手段は、前記コンテンツにおいて置き換えられたブロックデータを、読み出された前記部分データにより置き換えてもよい。

- [0018] この構成によれば、前記コンテンツをブロックごとに扱うことにより、所定長のブロックデータを確実に無効化することができる。

また、前記コンテンツを構成する各ブロックデータは、デジタル著作物が前記固定長毎に暗号化されて生成されたものであり、前記記録媒体には、抽出された前記部

分データを復号し、前記復号された部分データを前記記録媒体の媒体鍵を用いて暗号化した再暗号化データが記録されており、前記読出手段は、前記記録媒体から、前記部分データを読み出すのに代えて、前記再暗号化データを読み出し、前記再置換手段は、前記コンテンツのうち置き換えられたブロックデータを、読み出された前記部分データにより置き換えるのに代えて、前記再暗号化データを前記媒体鍵を用いて復号し、復号された前記再暗号化データに対し、前記デジタル著作物に施されたのと同じ暗号化を施して前記部分データを生成し、前記コンテンツにおいて置き換えられたブロックデータを、前記生成された部分データで置き換えてもよい。

[0019] また、前記記録媒体には、前記媒体鍵が記憶されており、前記再置換手段は、前記記録媒体から、前記媒体鍵を読み出す鍵読出部と、前記再暗号化データを前記媒体鍵を用いて復号する復号部と、復号された前記再暗号化データに対し、前記デジタル著作物に施されたのと同じ暗号化を施して前記部分データを生成する暗号化部と、前記コンテンツのうち置き換えられたブロックデータを、前記生成された部分データで置き換える置換部と、前記記録媒体に記憶されている媒体鍵を消去する鍵消去部とを含んでもよい。

[0020] この構成によれば、前記コンテンツを暗号化して扱うことができ、著作権をより強く保護できる。

また、前記記録媒体は、さらに、前記コンテンツにおける前記部分データの位置を記憶しており、前記読出手段は、さらに、前記記録媒体から前記位置を読み出し、前記再置換手段は、前記記憶手段に記憶されている前記コンテンツにおける前記位置のデータを、読み出された前記部分データにより置き換えてもよい。

[0021] この構成によれば、前記コンテンツを復元する場合に、前記記録媒体に書き込まれた、前記コンテンツにおける部分データの位置と、前記部分データを読み出し、前記コンテンツにおける前記位置に前記部分データを書き込むことで無効化された前記コンテンツを容易に復元することができる。

本発明のコンテンツ移動方法は、コンテンツを記憶している記憶手段を備え、前記コンテンツを可搬型の記録媒体に移動するコンテンツ移動装置において用いられるコンテンツ移動方法であって、前記コンテンツに、品質を下げる不可逆変換を施して

変換コンテンツを生成する生成ステップと、前記コンテンツの一部である部分データを抽出する抽出ステップと、前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換ステップと、生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込ステップとを含む。

[0022] この構成によれば、前記記憶手段に記憶されたコンテンツを再生できないよう無効化し、前記記録媒体に記録された変換コンテンツのみ再生可能として著作権を保護することができる。

また、前記部分データを、前記記憶手段に記憶されているコンテンツの前記無効化された部分に書き戻し、前記記録媒体に記録された変換コンテンツを消去すれば、著作権を保護しつつ、前記コンテンツ移動装置において、記録媒体に移動する前のコンテンツを復元することができる。

[0023] 本発明のコンピュータプログラムは、コンテンツを記憶している記憶手段を備え、前記コンテンツを可搬型の記録媒体に移動するコンテンツ移動装置において用いられるコンピュータプログラムであって、前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成ステップと、前記コンテンツの一部である部分データを抽出する抽出ステップと、前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換ステップと、生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込ステップとを含む。

[0024] 本発明の記録媒体は、コンピュータ読み取り可能な記録媒体であって、前記コンピュータプログラムを記録している。

この構成によれば、前記記憶手段に記憶されたコンテンツを再生できないよう無効化し、前記記録媒体に記録された変換コンテンツのみ再生可能として著作権を保護することができる。

[0025] また、前記部分データを、前記記憶手段に記憶されているコンテンツの前記無効化された部分に書き戻し、前記記録媒体に記録された変換コンテンツを消去すれば、著作権を保護しつつ、前記コンテンツ移動装置において、記録媒体に移動する前の

コンテンツを復元することができる。

本発明の記録媒体は、コンテンツに質を下げる不可逆変換を施された変換コンテンツと、前記コンテンツから抽出された部分データとを記録している。

[0026] 本発明のコンテンツ移動システムは、可搬型の記録媒体と、記憶しているコンテンツを前記記録媒体に移動するコンテンツ移動装置とから成るコンテンツ移動システムであって、前記コンテンツ移動装置は、コンテンツを記憶している記憶手段と、前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成手段と、前記コンテンツの一部である部分データを抽出する抽出手段と、前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換手段と、生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込手段とを含み、前記記録媒体は、前記変換コンテンツと前記部分データとを記録するための記憶領域を有する。

[0027] この構成によれば、前記記憶手段に記憶されたコンテンツを再生できないよう無効化し、前記記録媒体に記録された変換コンテンツのみ再生可能として著作権を保護することができる。

また、前記部分データを、前記記憶手段に記憶されているコンテンツの前記無効化された部分に書き戻し、前記記録媒体に記録された変換コンテンツを消去すれば、著作権を保護しつつ、前記コンテンツ移動装置において、記録媒体に移動する前のコンテンツを復元することができる。

図面の簡単な説明

[0028] [図1]本発明の実施形態に係るコンテンツ記録再生システムの概略構成を示す図である。

[図2]本発明の実施形態に係るHDレコーダ、SDカードの構成を示すブロック図である。

[図3]コンテンツのデータ構造の一例を示す図である。

[図4]コンテンツ記録部に記憶されるデータの一例を示す図である。

[図5]抽出処理が行われるデータの構成の一例を示す図である。

[図6]SDカードに記憶されるデータの一例を示す図である。

[図7]コンテンツのムーブ処理を示すフローチャートである。

[図8]コンテンツのムーブ処理を示すフローチャートである。

[図9]コンテンツのムーブ処理を示すフローチャートである。

[図10]コンテンツのムーブバック処理を示すフローチャートである。

[図11]装置間のムーブ処理を行うHDレコーダの構成の一例を示すブロック図である。
。

符号の説明

- [0029]
- 1 コンテンツ記録再生システム
 - 10 コンテンツ供給装置
 - 30 ネットワーク
 - 100 HDレコーダ
 - 101 装置記録鍵記憶部
 - 102 コンテンツ受信部
 - 103 暗号化部
 - 104 コンテンツ記録部
 - 105 暗号化コンテンツ読出部
 - 106 復号部
 - 107 変換部
 - 108 媒体記録鍵生成部
 - 109 暗号化部
 - 110 部分情報抽出部
 - 111 暗号化部
 - 112 復号部
 - 113 制御部
 - 114 再生制御部
 - 115 認証部
 - 116 書込読出部
 - 117 操作指示取得部

- 118 部分情報抽出部
- 120 モニタ
- 300 SDカード
- 301 認証部
- 302 変換コンテンツ記憶部
- 303 媒体記録鍵記憶部
- 304 部分情報記憶部
- 310 認証部
- 311 送受信部

発明を実施するための最良の形態

[0030] 以下、本発明の実施の形態を図示例と共に説明する。

<実施の形態1>

本発明に係る実施の形態1のコンテンツ記録再生システム1について、図を用いて説明する。

<コンテンツ記録再生システム1の概要>

本発明のコンテンツ記録再生システム1は、図1に示すようにコンテンツ供給装置10、ハードディスクレコーダ(以下、HDレコーダという。)100、HDレコーダ100に装着されるSDカード300、HDレコーダ400から構成される。コンテンツ供給装置10と、HDレコーダ100とはインターネットを介して接続され、HDレコーダ100及びHDレコーダ400は、IEEE1394に基づくネットワーク30により接続されている。

[0031] HDレコーダ100は、コンテンツ供給装置10から送信される映像データ、音声データ、制御用データを含むコンテンツを受信し、受信したコンテンツを自装置内のハードディスクに記憶する。

前記コンテンツは、MPEG2(Moving Picture Experts Group 2)仕様に基き作成されたトランスポートストリーム(以下、TSという。)であり、Copy One Generationが指定されたCCI(Copy Control Information)を含むものとする。

[0032] HDレコーダ100は、受信したコンテンツを自装置内に備えるハードディスクに記憶することもできるが、この場合、CCIを、コピー不可を示す「Copy No More」に設

定し直してから記憶する。

また、HDレコーダ100は、取得した前記コンテンツを、装着されたSDカード300にコピーすることは出来ないが、移動させることは可能である。しかし、SDカード300が備える記憶領域は、HDレコーダ100が備えるハードディスクの記憶領域よりも小さく、ハードディスクに記憶されているコンテンツを、SDカード300の記憶領域にそのまま記憶させることはできない。

[0033] この場合、HDレコーダ100は、ハードディスクに記憶されているMPEG2仕様に基づく高品位なコンテンツを、より圧縮率の高いMPEG4仕様に基づく低品位なコンテンツへとトランスコードし、コンテンツのデータ量を小さくしてから、SDカード300に記録し、また高品質なMPEG2仕様のコンテンツを無効化して使用不可能にし、保持しておく。

[0034] HDレコーダ100は、SDカード300に移動されたコンテンツを、自装置内のハードディスクへ再度移動し、当該コンテンツを再生することも可能であるが、この場合にも、コンテンツを低品位に再生せず、HDレコーダ100からSDカード300への移動を行う前と同じ、高品位に再生する。

<HDレコーダ100の構成>

HDレコーダ100は、図2に示すように、装置記録鍵記憶部101、コンテンツ受信部102、暗号化部103、コンテンツ記録部104、暗号化コンテンツ読出部105、復号部106、変換部107、媒体記録鍵生成部108、暗号化部109、部分情報抽出部110、暗号化部111、復号部112、制御部113、再生制御部114、認証部115、書込読出部116、操作指示取得部117から構成される。

[0035] HDレコーダ100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、HDレコーダ100は、その機能を達成する。

[0036] 装置記録鍵記憶部101は、ROMから構成され、HDレコーダ100に固有の鍵情報である装置記録鍵K1と、装置識別子「ID__A」とを記憶している。また、装置記録鍵

記憶部101は、保護機構を備えており、外部からの不正アクセスから保護されている。

前記装置記録鍵及び装置識別子は、予め、HDレコーダ100の出荷時に装置記録鍵記憶部101に書き込まれている。

- [0037] コンテンツ受信部102は、コンテンツ供給装置10から、DTCP(Digital Transmission Content Protection)規格で定められた手順に従い、コンテンツ及び前記コンテンツを識別するコンテンツ識別情報(以下、CID)を安全に受信し、受信したコンテンツ及びCIDを暗号化部103に送信する。

DTCP規格については、公知の技術で実現可能であるため、詳細については、言及しない。

- [0038] コンテンツ受信部102が受信するコンテンツであるTSは、一例として図3(a)に示すTSP(1)〜TSP(M)までのM(Mは自然数)個のTSパケット(以下、TSPという)から構成される。

コンテンツ受信部102は、TSP(1)から順に1つずつTSP(M)までのM個のTSPを受信し、TSPを受信する毎に暗号化部103へと出力する。

- [0039] また、コンテンツ受信部102は、TSから、MPEG2仕様にに基づき、PAT(Program Association Table)、PMT(Program Map Table)等の映像再生に必要な制御データを抽出し、抽出したPAT、PMT等を参照して、映像信号に関するデータの packets ID(以下、PIDという。)であるVPIDを読み出して制御部113に通知する。

- [0040] 暗号化部103は、制御部113から装置記録鍵読出指示を受信した場合に、装置記録鍵記憶部101から前記装置記録鍵を読み出し、コンテンツ受信部102から入力されるTSPを、所定のバイト数のデータである処理ブロック単位で暗号化し、暗号化された処理ブロックである暗号化ブロックと、コンテンツ受信部102から入力されるCIDとを対応づけてコンテンツ記録部104に書き込む。

- [0041] 暗号化部103は、前記暗号化を、前記装置記録鍵を用いて前記処理ブロックに暗号アルゴリズムE1を施すことで行う。

ここで、処理ブロックは512バイト長のデータとする。

暗号化部103は、コンテンツ受信部102から一例として図3(a)に示すように、TSP

(1)から順にTSP(2)・・・TSP(M)までのM(Mは自然数)個のTSPが入力される場合、入力されるTSPを、図3(b)に示すように、それぞれが512バイトのデータである処理ブロック151〜処理ブロック15N(Nは自然数)に区切って、各処理ブロックそれぞれを暗号化する。

[0042] 処理ブロック151は、188バイトのTSP(1)と、188バイトのTSP(2)と、TSP(3)の前半136バイトとからなり、処理ブロック152は、TSP(3)の後半52バイトと、188バイトのTSP(4)と、188バイトのTSP(5)と、TSP(6)の前半84バイトとから成る。

以下、処理ブロック151をC1(1)といい、処理ブロック152をC1(2)といい、同様に、処理ブロック15NをC1(N)という。

[0043] 暗号化部103は、例えば、前記装置記録鍵を用いてC1(1)に対し暗号アルゴリズムE1を施して、暗号文である暗号化ブロックEC1(1)を生成し、生成したEC1(1)を、暗号化ブロックに係るCIDとを対応づけてコンテンツ記録部104に書き込む。

暗号化部103は、上述のC1(1)の場合と同様にして、図3(a)に示すTSを、図3(b)で示す処理ブロック毎に暗号化し、結果として得る図3(c)に示す暗号化ブロック161〜暗号化ブロック16N(Nは自然数)をコンテンツ記録部104に書き込む。暗号化ブロック161(EC1(1))は、処理ブロック151(C1(1))が暗号化されたものであり、暗号化ブロック162(EC1(2))は、処理ブロック152(C1(2))が暗号化されたものであり、暗号化ブロック16N(EC1(N))は、処理ブロック15N(C1(N))が暗号化されたものである。

[0044] ここで、以下、各処理ブロックにおける先頭の処理ブロックを基点とする位置、及び、各暗号化ブロックにおける先頭の暗号化ブロックを基点とする位置をブロック番号という。

例えば、C1(2)のブロック番号は「2」であり、C1(3)のブロック番号は「3」であり、C1(N)のブロック番号は「N」である。同様に、EC1(2)のブロック番号は「2」であり、EC1(3)のブロック番号は「3」であり、C1(N)のブロック番号は「N」である。

[0045] また、暗号化部103は、復号部112から、CIDとブロック番号と処理ブロックの連結データとを受信可能であり、前記連結データを受信した場合に、前記装置記録鍵を用い、連結データに含まれる処理ブロックに対し暗号アルゴリズムE1を施して、暗号

文を生成し、生成した暗号文を、受信したCIDに対応する前記連結データに含まれるブロック番号と同じブロック番号を持つコンテンツ記録部104に記録されている処理ブロックに上書きする。

[0046] 例えば、CID「1」とブロック番号「2」と、処理ブロック「C2(2)」の連結データを、復号部112から受信した場合、暗号化部103は、前記装置記録鍵を用いC2(2)に対し暗号アルゴリズムE1を施して暗号文である暗号化ブロックEC(2)を生成し、コンテンツ記録部104におけるCIDが「1」、ブロック番号が「2」の位置に、EC(2)を上書きする。

[0047] これにより、コンテンツ記録部104において、無効化されていた、CID「1」、ブロック番号「2」の位置のデータが、無効化前のデータに置き換わる。

コンテンツ記録部104は、ハードディスクユニットから構成され、暗号化部103により書き込まれるCIDと、暗号化ブロック群である暗号化コンテンツとを対応づけて保持する。

[0048] コンテンツ記録部104は、一例として、図4に示すように、値が「1」であるCID171と、EC1(1)〜EC1(N)までのN個の暗号化ブロックから成る暗号化コンテンツとを対応づけて保持している。

暗号化コンテンツ読出部105は、制御部113からCIDを含む読み出し指示を受信し、コンテンツ記録部104に記録された、前記読み出し指示に含まれるCIDに対応づけられている暗号化ブロックを、ブロック番号の早い順に1つずつ読み出して、復号部106に送信する。

[0049] 復号部106は、HDDレコーダの電源投入時に、装置記録鍵記憶部101から、前記装置記録鍵を読み出しておき、暗号化コンテンツ読出部105から、暗号化ブロックを1つずつ受信すると、前記装置記録鍵を用いて、受信した暗号化ブロックに対し、復号アルゴリズムD1を施して、復号文である処理ブロックを生成し、生成した処理ブロックを、変換部107と、部分情報抽出部110と、再生制御部114とに出力する。

[0050] 例えば、復号部106は、暗号化コンテンツ読出部105から、EC1(1)を受信した場合、復号部106は、前記装置記録鍵を用いてEC1(1)に復号アルゴリズムD1を施して、C1(1)を生成し、C1(1)を変換部107と、部分情報抽出部110に出力する。

ここで、復号アルゴリズムD1は、暗号アルゴリズムE1により生成された暗号文を復号するアルゴリズムである。

- [0051] 変換部107は、復号部106から受信する処理ブロックから成るMPEG2仕様で符号化されたコンテンツを、MPEG4仕様で符号化されたコンテンツ(以下、変換コンテンツという。)へと変換し、前記変換コンテンツを暗号化部109に送信する。

例えば、変換部107は、復号部106から、処理ブロックC1(1)、C1(2)、C1(3)・・・C1(N)を順に受信し、受信した処理ブロックで、MPEG4仕様へとトランスコード可能であるか否か判定する。前記判定は、例えば、MPEG2仕様に基づく、Iピクチャなどのピクチャが復号可能となったか否かにより行い、ピクチャが復号可能となればトランスコード可能であると判定し、当該ピクチャを構成する処理ブロックをまとめてMPEG4へとトランスコードしていくことにより、MPEG4仕様の変換ブロックC2(1)、C2(2)・・・C2(F)(Fは自然数)を生成する。

- [0052] 媒体記録鍵生成部108は、制御部113からの、装置識別子とCIDとを含む、変換コンテンツ用の媒体記録鍵の生成指示を示す第1生成指示を受信し、擬似乱数を用いて媒体記録鍵KT4を生成し、暗号化部109に送信する。また、KT4を後述するSDカード300の媒体記録鍵記憶部303に書き込み、媒体記録鍵生成部108内に残存するKT4を消去する。

- [0053] また、媒体記録鍵生成部108は、制御部113からの、装置識別子とCIDとを含む、部分情報用の媒体記録鍵の生成指示を示す第2生成指示を受信し、擬似乱数を用いて媒体記録鍵KT2を生成し、暗号化部111に送信する。また、KT2を後述するSDカード300の媒体記録鍵記憶部303に書き込み、媒体記録鍵生成部108内に残存するKT2を消去する。

- [0054] 暗号化部109は、媒体記録鍵生成部108から、装置識別子とCIDとKT4を受信し、変換部107から前記変換コンテンツを受信すると、前記変換コンテンツにおける所定長のデータである変換ブロック毎にKT4を用いて暗号アルゴリズムE2を施して暗号化変換ブロックを生成し、当該暗号化変換ブロックと、装置識別子とCIDとを対応づけて、後述するSDカード300内の変換コンテンツ記憶部302に書き込む。

- [0055] 部分情報抽出部110は、復号部106から、逐次受信する処理ブロックの中から、処

理ブロック中のTSPのパケットIDと、Iピクチャの先頭部分に含まれる値が「1」であるPCTフラグとを目印に、Iピクチャの先頭512バイトのデータを含む処理ブロックを抽出する。

一例として、図5に示すように、C1(1)〜C1(7)の各処理ブロックが、順に部分情報抽出部118に入力される場合について説明する。

[0056] ここで、部分情報抽出部110は、CIDとVPIDを制御部113から受信しており、映像データが符号化されたTSPのパケットID(以下、PIDという。)は、値「VPID」であるものとする。

まず、部分情報抽出部110は、入力される処理ブロックが、PID=VPIDであるTSPを含むか否かを判定し、含まない場合には当該処理ブロックを破棄し、含む場合には、さらに、当該TSPが、値が「1」であるPCTを含むか否かを判定する。

[0057] 処理ブロックが、PID=VPIDかつPCTが「1」であるTSPを含む場合、処理ブロックのブロック番号で示される暗号化ブロックを無効データで上書きし、当該処理ブロックに含まれる該当TSPのバイト数を無効化バイト数として保持する。

図5の場合、C1(2)が、PID=VPIDかつPCTが「1」であるTSP(5)を含むので、TSP(5)を含む処理ブロックのブロック番号である「2」と、同じブロック番号を持ち、コンテンツ記録部104に記録されている暗号化ブロックであるEC1(2)を、無効データで上書きする。

[0058] この時、処理ブロックC1(2)には、TSP(5)が188バイト含まれるので、前記無効化バイト数を188とする。

次に、部分情報抽出部110は、入力される処理ブロックが、PID=VPIDであるTSPを含むか否かを判定する。

、PID=VPIDであるTSPを含まない場合には、当該処理ブロックを破棄し、含む場合には、コンテンツ記録部104に記録され当該処理ブロックのブロック番号で示される暗号化ブロックを無効データで上書きし、当該処理ブロックに含まれる該当TSPのバイト数を無効化バイト数として保持する。

[0059] また、前記処理ブロックのブロック番号と、前記処理ブロックとを連結し、連結結果である部分ブロックを、暗号化部111に送信する。

ここで、ブロック番号がLである処理ブロックC1(L)の部分ブロックをPC1(L) (Lは自然数)と記し、PC1(L)を(L || C1(L))と示す。記号「||」は連結を示す。

[0060] 例えば、前記該当する処理ブロックがC1(2)である場合、部分ブロックPC1(2)=(2 || C1(2))である。

上記のようなPID=VPIDであるTSPを含む処理ブロックは、C1(4)と、C1(6)が該当する。

C1(4)について、部分情報抽出部110は、C1(4)のブロック番号である「4」と、同じブロック番号を持ち、コンテンツ記録部104に記録されている暗号化ブロックであるEC1(4)を、無効データで上書きし、C1(4)に含まれるTSP(10)のバイト数である188バイトを、前記無効化バイト数に加算する。

[0061] また、部分情報抽出部110は、PC1(4)=(4 || C1(4))を暗号化部111に送信する。

同様に、C1(6)について、部分情報抽出部110は、C1(6)のブロック番号である「6」と、同じブロック番号を持ち、コンテンツ記録部104に記録されている暗号化ブロックであるEC1(6)を、無効データで上書きし、C1(6)に含まれるTSP(10)のバイト数である188バイトを、前記無効化バイト数に加算する。

[0062] また、部分情報抽出部110は、PC1(6)=(6 || C1(6))を暗号化部111に送信する。

ここで、前記無効化バイト数は、564バイトとなり、512バイト以上となったので、部分情報抽出部110は、前記無効化バイト数を0バイトにクリアし、前述のPID=VPIDかつPCTが「1」であるTSPを含む処理ブロックか否かの判定処理に戻る。

[0063] 以上の処理により、Iピクチャに該当する映像データの先頭から512バイト以上を含む処理ブロックを選出して、無効化することができる。

暗号化部111は、媒体記録鍵生成部108から装置識別子とCIDとKT2を受信し、また部分情報抽出部110から部分ブロックを受信すると、KT2を用いて、受信した部分ブロックに暗号アルゴリズムE3を施して暗号化部分ブロックを生成し、当該暗号化部分ブロックと、装置識別子とCIDとを対応づけて後述するSDカード300内の部分情報記憶部304に書き込む。

[0064] ここで、以下、部分ブロックPC1(L)が暗号化された結果である暗号化部分ブロックを、EPC1(L)という。

復号部112は、制御部113からCIDと装置識別子とを含む部分情報読出指示を受信可能であり、前記部分情報読出指示を受信すると、後述するSDカード300内の媒体記録鍵記憶部303に記憶されている、前記部分情報読出指示に含まれるCIDと装置識別子とに対応するKT2を読み出す。また、復号部112は、後述するSDカード300内の部分情報記憶部304に記憶されている、前記部分情報読出指示に含まれるCIDと装置識別子とに対応する暗号化部分ブロックを、ブロック番号の早い順に1つずつ読み出し、KT2を用いて、読み出した暗号化部分ブロックに復号アルゴリズムD3を施して、ブロック番号と処理ブロックの結合物である部分ブロックを復元し、復元された部分ブロックを暗号化部103に送信する。

[0065] ここで、復号アルゴリズムD3は、暗号アルゴリズムE3により生成された暗号文を復号するアルゴリズムである。

例えば、復号部112は、部分情報記憶部304から、暗号化部分ブロックEPC1(L)を読み出した場合、KT2を用いてEPC1(L)に復号アルゴリズムD3を施して、 $PC1(L) = (L \parallel C1(L))$ を生成し、PC1(L)を暗号化部103に送信する。

[0066] 制御部113は、HDレコーダ100の全体動作を制御する。

制御部113は、装置記録鍵と装置識別子とを、電源投入時に、装置記録鍵記憶部101から読み出して、保持しておく。

制御部113は、操作指示取得部117から、操作指示情報を受信し、受信した操作指示情報に対応した処理を行う。

[0067] 制御部113は、操作指示取得部117から、ムーブすべきコンテンツのCIDを含む、コンテンツのムーブを示す操作指示情報を受信した場合に、認証部115に対し、認証指示を送信し、認証部115による相互認証処理が成功した場合、さらに、暗号化コンテンツ読出部105に対して、CIDを含む読み出し指示を送信し、また、媒体記録鍵生成部108に対し、装置識別子「ID_A」とCIDとを含む、変換コンテンツ用の媒体記録鍵の生成指示を示す第1生成指示と、装置識別子「ID_A」とCIDとを含む、部分情報用の媒体記録鍵の生成指示を示す第2生成指示を送信し、また、部分情報

抽出部110に対して、VPIDを通知する。

- [0068] また、制御部113は、前記VPIDをコンテンツ受信部102から受信した場合には、コンテンツ記録部104に保持しておく。

また、制御部113は、操作指示取得部117から、再生すべきコンテンツのCIDを含むコンテンツの再生を示す操作指示情報を受信した場合に、暗号化コンテンツ読出部105に対してCIDを含む読み出し指示を送信し、また、再生制御部114に対し、コンテンツの再生指示を送信する。

- [0069] 制御部113は、操作指示取得部117からムーブバックすべきコンテンツのCIDを含む、ムーブバックを示す操作指示情報を受信した場合、認証部115に認証指示を送信する。

制御部113は、認証部115から前記認証指示に対する認証処理の結果を受信し、前記認証処理が成功した場合には、暗号化部103に対し、装置記録鍵読出指示を送信し、また、媒体記録鍵記憶部303に記憶されている、装置識別子「ID__A」とCIDとに対応づけられたKT4を消去し、変換コンテンツ記憶部302に記憶されている、装置識別子「ID__A」とCIDとに対応づけられた変換コンテンツを消去し、復号部112に対し、装置識別子「ID__A」とCIDとを含む部分情報読出指示を送信する。

- [0070] 認証処理が失敗した場合には、制御部113は処理を終了する。

再生制御部114は、MPEGデコード回路と、DA(Digital to Analog)コンバータから成り、コンテンツ受信部102及び復号部106から、TSをTSP単位で受信する。

前記MPEGデコード回路は、受信したTSを、MPEG2仕様にに基づき、圧縮前の映像、音声を表すデジタル信号に復号し、復号された前記デジタル信号をDAコンバータで映像、音声を表すアナログ信号に変換して、モニタ120に出力する。

- [0071] MPEG2については、公知の技術であるので、説明を省略する。

認証部115は、制御部113からSDカード300に対する認証指示を受信し、SDカード300と相互認証処理を行い、認証処理の結果を制御部113に送信する。

SDカード300との間の相互認証処理が成功した場合に、以後、SDカード300は、HDレコーダ100に対するデータの書き込みを許可する。

- [0072] 認証部115は、前記相互認証処理を、例えば、CPRM(Content Protection f

or Recordable Media)仕様に基づき行う。CPRMについては、公知技術であり、特に説明は行わない。

書込読出部116は、SDカード300への情報の読み出し及び書き込みを行う。

操作指示取得部117は、電源ボタン、録画ボタン、ムーブボタン、受信チャンネル指定ボタン、メニューボタン、選択ボタン、カーソル移動ボタン、コンテンツID選択ボタンなどの各種ボタン及びリモートコントローラの受信回路を備える。

[0073] 利用者によるボタン操作及びリモートコントローラの操作を受け付け、受け付けた、ボタン操作及びリモートコントローラの操作を示す操作指示情報を制御部113へ出力する。

モニタ120は、スピーカ、ディスプレイを内蔵するテレビ受信機であり、再生制御部114から映像信号を受け取り、水平同期信号、垂直同期信号に基づき、映像をディスプレイに表示し、再生制御部114から、音声信号を受け取り、受け取った音声信号を音声に変換し、スピーカに出力する。

<SDカード300の構成>

SDカード300は、図2に示すように、認証部301と、変換コンテンツ記憶部302と、媒体記録鍵記憶部303と、部分情報記憶部304とから構成される。

[0074] ここで、SDカード300内の記憶領域は、セキュアな記憶領域と、非セキュアな記憶領域とから構成されており、具体的には、媒体記録鍵記憶部303はセキュアな記憶領域であり、変換コンテンツ記憶部302及び部分情報記憶部304は非セキュアな記憶領域である。

SDカード300は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、SDカード300は、その機能を達成する。

[0075] 認証部301は、HDレコーダ100内の認証部115からの要求に従い、認証部115との間で相互認証処理を行う。

前記相互認証処理が成功した場合に、認証部301は、以後、HDレコーダ100に対し、セキュアな記憶領域である媒体記録鍵記憶部303に対するデータの書き込み

、データの読み出しを許可する。

- [0076] 変換コンテンツ記憶部302は、暗号化部109により書き込まれる変換コンテンツを記憶する。

例えば、図6に示すように、装置識別子ID__A(165)とCID166と、EC2(1)〜EC2(F)のF個の暗号化変換ブロックとを対応づけて保持する。

媒体記録鍵記憶部303は、媒体記録鍵生成部108により書き込まれる、図6に示すような、装置識別子ID__A(335)とCID336と媒体記録鍵KT2(331)及びKT4(332)とを対応づけて記憶する。

- [0077] 部分情報記憶部304は、例えば、図6に示すように、装置識別子ID__A(355)とCID356と、PEC1(1)〜PEC1(G)のG(Gは自然数)個の暗号化変換ブロックとを対応づけて保持する。

<動作>

コンテンツ記録再生システム1の動作について、コンテンツのHDレコーダ100からSDカード300への(1)ムーブ処理、(2)ムーブしたコンテンツのSDカード300からHDレコーダ100へのムーブバック処理の順に説明する。

(1)ムーブ処理

前述のコンテンツ記録部104に記憶されたコンテンツを、SDカード300にムーブする処理について、図7〜9を用いて説明する。

- [0078] ここで、コンテンツ記録部104には、暗号化されたコンテンツとして図4に示すように、CID「1」(171)とEC1(1)〜EC1(N)とが対応づけて記録されており、SDカード300における変換コンテンツ記憶部302、媒体記録鍵記憶部303、部分情報記憶部304にはデータが記録されていないものとする。

ユーザは、リモートコントローラを操作することにより、コンテンツのムーブを指示する。

- [0079] 操作指示取得部117は、ムーブすべきコンテンツのCIDを含むムーブ指示を示す操作指示情報を制御部113に送信する(ステップS301)。

制御部113は、認証部115に対し、SDカード300との認証指示を送信する。

認証部115は、SDカード300の認証部301との間で相互認証処理を行い、制御

部113に認証結果を通知する(ステップS302)。

[0080] 相互認証が失敗した場合(ステップS303:NO)、処理を終了する。

相互認証が成功した場合(ステップS303:YES)、制御部113は、媒体記録鍵生成部108に対し、予め、装置記録鍵記憶部101から読み出している装置識別子「ID__A」と操作指示情報に含まれるCIDとを含む、第1生成指示を送信する。媒体記録鍵生成部108は、前記第1生成指示を受信し、媒体記録鍵KT4を生成し、ID__AとCIDとKT4を暗号化部109に送信する(ステップS304)。

[0081] 制御部113は、媒体記録鍵生成部108に対し、ID__AとCIDとを含む第2生成指示を送信する。媒体記録鍵生成部108は、前記第2生成指示を受信し、媒体記録鍵KT2を生成し、ID__AとCIDとKT2を暗号化部111に送信する(ステップS305)。

制御部113は、部分情報抽出部110に対し、CIDとVPIDを通知する(ステップS306)。

[0082] 制御部113は、暗号化コンテンツ読出部に対し、読出指示を送信する(ステップS307)。

暗号化コンテンツ読出部105は、制御部113から前記読出指示を受信し、内部変数iを「1」で初期化する(ステップS308)。

部分情報抽出部110は、VPIDを受信し、内部変数jを「1」に初期化し、kを「0」に初期化する(ステップS309)。

[0083] 暗号化コンテンツ読出部105は、内部変数iが、コンテンツ記録部104に記録されている暗号化ブロックの数より大きいかな否かを判定する(ステップS310)。

iが暗号化ブロックの数より大きい場合(ステップS310:YES)、暗号化コンテンツ読出部105は、媒体記録鍵生成部108に媒体記録鍵書込指示を送信する。

媒体記録鍵生成部108は、ID__Aと、CIDと、KT4と、KT2とを媒体記録鍵記憶部303に書き込み(ステップS311)、媒体記録鍵生成部108内に残存するKT4とKT2とを削除して、処理を終了する。

[0084] iが暗号化ブロックの数より小さい場合(ステップS310:NO)、暗号化コンテンツ読出部105は、コンテンツ記録部104からEC1(i)を読み出し、読み出したEC1(i)を復号部106に送信する(ステップS312)。

復号部106は、装置記録鍵K1を用い、EC1(i)を復号アルゴリズムD1により復号してC1(i)を生成し、生成したC1(i)を、部分情報抽出部110と、変換部107に送信する(ステップS313)。

- [0085] 部分情報抽出部110は、C1(i)を受信し、受信したC1(i)がPID=VPIDであるTSPを含むか否かを判定する(ステップS321)。

C1(i)が、PID=VPIDであるTSPを含まない場合(ステップS321:NO)、iを1インクリメントし(ステップS314)、ステップS310に移行する。

C1(i)が、PID=VPIDであるTSPを含む場合(ステップS321:YES)、部分情報抽出部110は、kが「0」か否かを判定する(ステップS322)。

- [0086] kが「0」でない場合(ステップS322:NO)、後述するステップS324に移行する。

kが「0」である場合(ステップS322:YES)、PID=VPIDであるTSPが、値が「1」であるPCTを含むか否かを判定する(ステップS323)。

値が「1」であるPCTを含まない場合(ステップS323:NO)、ステップS314に移行する。

- [0087] 値が「1」であるPCTを含む場合(ステップS323:YES)、部分情報抽出部110は、 $PC1(i) = (i \parallel C1(i))$ を暗号化部111に送信する。

暗号化部111は、KT2を用いPC1(i)に暗号アルゴリズムE3を施してPEC1(i)を生成する(ステップS324)。

暗号化部111は、PEC1(i)を部分情報記憶部304に書き込む(ステップS325)。

- [0088] ただし、ID__AとCIDとが部分情報記憶部304に書き込まれていない場合には、ID__AとCIDとPEC1(i)とを対応づけて書き込む。

部分情報抽出部110は、コンテンツ記録部104に記録されている、CIDに対応するEC1(i)をヌルデータで上書きする(ステップS326)。

部分情報抽出部110は、C1(i)に含まれる、PID=VPIDであるTSPのバイト数をkに加える(ステップS327)。

- [0089] 部分情報抽出部110は、kが512より大きいかな否かを判定する(ステップS328)。

kが512より大きい場合(ステップS328:YES)、kを「0」で初期化し(ステップS329)、ステップS314に移行する。

kが512より小さい場合(ステップS328:NO)、ステップS314に移行する。

- [0090] また、ステップS313において、復号部106から送信されたC1(i)を、変換部107は受信し(ステップS341)、これまでに復号部106から受信し保持しているデータに基づき、トランスコードが可能か否かを判定する(ステップS342)。

トランスコード不可能な場合(ステップS342:NO)、変換部107は、次のデータを復号部106から受信するのを待つ(ステップS347)。

- [0091] トランスコードが可能な場合(ステップS342:YES)、変換部107は、所定のデータ単位毎にトランスコードを実行し、結果として変換ブロックC2(j)を生成し(ステップS343)、C2(j)を暗号化部109に送信する。

暗号化部109は、C2(j)を受信し、KT4を用いC2(j)に暗号アルゴリズムE2を施し、EC2(j)を生成する(ステップS344)。

- [0092] 暗号化部109は、変換コンテンツ記憶部302に、ID__AとCIDとに対応づけてEC2(j)を書き込む(ステップS345)。

ただし、ID__AとCIDとが変換コンテンツ記憶部302に書き込まれていない場合には、ID__AとCIDとEC2(j)とを対応づけて書き込む。

変換部107は、jを「1」インクリメントし(ステップS346)、ステップS347に移行する。

- [0093] 以上の処理により、SDカード300の変換コンテンツ記憶部302には、図6に示すように、ID__A165とCID166とEC2(1)〜EC2(F)までのF(Fは自然数)個の変換ブロックとが対応づけて記憶され、媒体記録鍵記憶部303には、ID__A335とCID336とKT2(331)とKT4(332)が対応づけて記憶され、部分情報記憶部304は、ID__A355とCID356とPEC1(1)〜PEC1(G)のG(Gは自然数)個の暗号化部分ブロックとが対応づけて記憶されることとなる。

- [0094] なお、ID__A165、ID__A335、ID__A355は、同じ値を持つ装置識別子であり、CID166、CID336、CID356は、同じ値を持つコンテンツ識別情報である。

(2) ムーブバック処理

前述の(1)ムーブ処理によって、HDレコーダ100からSDカード300へとムーブされたコンテンツを、SDカード300からHDレコーダ100へとムーブバックする処理について、図10を用いて説明する。

[0095] ユーザは、リモートコントローラを操作することにより、ムーブされたコンテンツのムーブバックを指示する。

操作指示取得部117は、ムーブバックすべきコンテンツのCIDを含むムーブバック指示を示す操作指示情報を制御部113に送信する(ステップS401)。

制御部113は、操作指示取得部117から、前記ムーブバック指示を示す操作指示情報を受信し、認証部115に認証指示を送信する。

[0096] 認証部115は、認証部301との間で、相互認証処理を実行する(ステップS402)。

相互認証処理が失敗した場合(ステップS403:NO)、制御部113は、処理を終了する。

相互認証処理が成功した場合(ステップS403:YES)、制御部113は、暗号化部103に対し、装置記録鍵読出指示を送信し、また、媒体記録鍵記憶部303に記憶されている、CID、ID__Aに対応するKT4を消去する(ステップS404)。

[0097] 制御部113は、変換コンテンツ記憶部302に記憶されている、CID、ID__Aに対応する変換コンテンツを消去する(ステップS405)。

暗号化部103は、装置記録鍵読出指示を受信すると、装置記録鍵記憶部101から装置記録鍵K1を読み出す(ステップS406)。

制御部113は、復号部112に対し、ID__A、CIDを含む部分情報読出指示を送信する(ステップS407)。

[0098] 復号部112は、媒体記録鍵記憶部303から、ID__A、CIDに対応するKT2を読み出す(ステップS408)。

復号部112は、内部変数iを「1」で初期化する(ステップS409)。

復号部112は、部分情報記憶部304から、ID__A、CIDに対応するPEC1(i)を読み出す(ステップS410)。

[0099] 復号部112は、KT2を鍵としてPEC1(i)に復号アルゴリズムD3を施してPC1(X) = (X || C2(X))を復元し、CIDとPC1(X)とを暗号化部103に送信する(ステップS411)。

暗号化部103は、PC1(X)を受信し、PC1(X)からC2(X)を取り出し、K1を鍵としてC1(X)に暗号アルゴリズムE1を施し、EC1(X)を生成する(ステップS412)。

[0100] 暗号化部103は、コンテンツ記録部104内の、CIDに対応し、ブロック番号がXである、無効化されたデータを、EC1(X)で上書きする(ステップS413)。

制御部113は、部分情報記憶部304内の、ID__AとCIDとに対応するPEC(i)を消去する(ステップS414)。

復号部112は、iが(部分情報記憶部内の暗号化ブロック数)より大きいかな否かを判定する(ステップS415)。

[0101] iが(部分情報記憶部内の暗号化ブロック数)より大きいと判定した場合(ステップS415: YES)、ムーブバック処理を終了し、iが(部分情報記憶部内の暗号化ブロック数)以下であった場合(ステップS415: NO)、iを1インクリメントして(ステップS416)、ステップS410に移行する。

また、ムーブバック処理の終了時に、制御部113は、変換コンテンツ記憶部302に記憶されているID__A165とCID166を消去し、媒体記録鍵記憶部303に記憶されているID__A335とCID336を消去し、部分情報記憶部304に記憶されているID__A355とCID356を消去する。

(その他の変形例)

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

[0102] (1) 本実施形態では、SDカードからHDレコーダへコンテンツをムーブバックする場合に、SDカードに記録されている変換コンテンツ、媒体記録鍵KT4を消去する構成としたが、本発明はその構成に限定されるものではない。

例えば、SDカードに記録された変換コンテンツを消去せずに、変換コンテンツの復号に必要なKT4だけを消去して、前記変換コンテンツを利用不可状態にする構成であってもよい。また、変換コンテンツを全て消去する代わりに、変換コンテンツの一部を破壊して利用できない状態にする構成であってもよい。

[0103] (2) HDレコーダは、さらに、ムーブ処理の進行状況を記憶する状態記憶部を備える構成であってもよい。

例えば、HDレコーダは、SDカードへのコンテンツのムーブが正しく完了しなかった

場合に、前記状態記憶部に記憶する進行状況に基づいて、コンテンツのムーブ処理を続けて行うか、コンテンツのムーブ処理を最初からやり直すかを判断する構成であってもよい。

[0104] さらに、HDレコーダは、前記状態記憶部に記憶する進行状況を利用者に通知する通知部を備える構成であってもよい。その場合、ムーブ処理が正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツのムーブ処理を続けるか、あるいはコンテンツのムーブ処理を最初からやり直すかの指示を受け、当該指示に基づくムーブ処理を実行する構成としてもよい。

[0105] (3) 本実施形態において、HDレコーダからSDカードへと鍵を移動し、移動した後にHDレコーダに残存する当該鍵を消去する場合において、鍵の受信側であるSDカードが当該鍵を受け取り記録領域に記録した後に、鍵の送信側であるHDレコーダに対し鍵の記録が完了したことを通知し、当該通知を受けてから、HDレコーダが自装置内に残存する前記鍵を消去する構成としてもよい。

[0106] (4) 本実施形態において、コンテンツには前記コンテンツを一意に識別するための識別子が付与されており、HDレコーダはSDカードにコンテンツをムーブする場合に前記識別子を記録しておき、SDカードにムーブされたコンテンツを自身の記録領域に書き戻す場合に、自身が保持する識別子及びSDカードに記録されているコンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツをHDレコーダに書き戻す構成としてもよい。

[0107] また、コンテンツには、コンテンツを一意に識別する識別子の代わりに、移動元の装置を一意に識別する識別子が付与されている構成であってもよい。この場合、HDレコーダは、コンテンツに付与されている移動元の装置の識別子と、自身が保持している自装置の識別子とが一致するか否かを判定して、一致した場合に限り、コンテンツをSDカードから書き戻す構成であってもよい。

[0108] (5) 本発明の実施の形態では、HDレコーダは、部分ブロックを媒体記録鍵で暗号化してSDカードに書き込む構成としたが、当該構成に限定されるものではない。前記部分ブロックを装置記録鍵で暗号化して記録する構成であってもよいし、別の鍵を新たに生成して暗号化して記録する構成であってもよい。

(6)実施の形態中では、暗号アルゴリズムE1、E2、E3、復号アルゴリズムD1、D2、D3について、具体的に特定していないが、例えば、DES(Data Encryption Standard)や、AES(Advanced Encryption Standard)等の一般的に用いられる暗号方式に従い暗号化、復号処理を行えばよい。

[0109] また、HDレコーダとSDカードの間の認証処理、通信処理については、一般的に行われているCPRM規格に基づいて行えばよいし、著作権保護が可能である他の規格に基づいて行ってもよい。

同様に、複数のHDレコーダ間の認証処理、通信処理についても、一般的に行われているDTCP規格に基づいて行えばよいし、著作権保護が可能である他の規格に基づいて行ってもよい。

[0110] (7)本実施形態では、コンテンツは、TSの形式で、コンテンツ供給装置からHDレコーダへと供給される構成としたが、これに限らない。

例えば、HDレコーダがチューナー等の放送受信部を備え、コンテンツ供給装置から衛星を介した放送波を用いてコンテンツを送出し、HDレコーダが前記放送波を受信して、受信した放送波からコンテンツを復元することとしてもよい。

[0111] また、HDレコーダが、DVD(Digital Versatile Disc)、BD(Blu-ray Disc)等、コンテンツを記録している記録媒体からコンテンツを読み出す構成であってもよい。

(8)HDレコーダは、MPEG2仕様により符号化されたコンテンツを保持しており、SDカードへは、前記コンテンツをMPEG4仕様により符号化されたコンテンツにトランスコードした上で、SDカードに書き込むこととしていたが、これに限らない。

[0112] 例えば、当該変換は常に行う必要はなく、SDカードの記憶容量が大きく、コンテンツをそのまま記憶出来る場合はMPEG2からMPEG4への変換を行わなくてもよいし、SDカードの記憶容量の未使用領域のサイズを、HDレコーダがムーブ処理の前に算出し、未使用領域のサイズがコンテンツのサイズより小さい場合に、前記変換処理を行うなど、SDカードの記憶領域の容量残量などの条件に従い、変換を実行するかどうかを判定した上で、ムーブ処理を行うこととしてもよい。

[0113] また、移動前及び移動後のコンテンツの符号化方式は、MPEG2及びMPEG4に限る必要はない。

移動前のコンテンツを符号化する符号化方式よりも、移動後のコンテンツの符号化方式の方が、圧縮率が高ければよい。

例えば、HDレコーダでは、前記コンテンツをMPEG4仕様にに基づき符号化して記録しておき、SDカードには、MPEG7仕様にに基づきトランスコードした上でコンテンツを書き込むこととしてもよい。

- [0114] また、HDレコーダが保持しているMPEG2仕様にに基づくコンテンツにおける、画像フレームの解像度に応じて、ムーブ処理時にトランスコードするか否かを判定してもよい。

例えば、画像フレームの解像度がVGA (Video Graphics Array) より大きい場合に、前記トランスコードを実行し、VGA以下である場合に、前記トランスコードを実行せずに、前記コンテンツを、HDレコーダからSDカードへと移動することとしてもよい。

- [0115] (9) Iピクチャの先頭512バイトを無効化する例で説明したが、これには限らない。

コンテンツ記憶部に記憶されているコンテンツが、正常に再生されないように処理されていればよい。

例えば、PCTが「1」であるTSPを含み、PIDが同じVPIDである連続する数個、例えば3つのTSPを無効化することとしてもよい。

- [0116] また、先頭に限らず、Iピクチャの所定位置を無効化することとしてもよいし、Iピクチャ全てを無効化してもよいし、無効化するデータは、連続データでなく散在するものとしてもよい。

また、無効化するデータはIピクチャに限るものではなく、Pピクチャも合わせて無効化してもよいし、例えば、PAT、PMT等の選局に用いるデータを無効化してもよい。

- [0117] また、コンテンツ内の決まった位置、例えば、処理ブロックにおける先頭から64バイトと、449バイト目から512バイト目などを無効化することとしてもよい。

(10) 本実施形態では、HDレコーダは、処理ブロックと、そのコンテンツにおける位置であるブロック番号とを連結して部分ブロックを生成し、さらに前記部分ブロックを暗号化して暗号化部分ブロックを生成し、SDカードに書き込んでいるが、これには限らない。

[0118] 例えば、前記ブロック番号はコンテンツ記憶部に記憶しておき、前記ブロック番号に対応する処理ブロックを暗号化してSDカードに書き込むこととしてもよい。

この場合、HDレコーダは、SDカードから前記暗号化されて処理ブロックを読み出して、復号して処理ブロックを復号し、前記ブロック番号をコンテンツ記憶部から読み出して、前記処理ブロックを、デバイス鍵で暗号化し、前記ブロック番号が示す位置に対応する部分に上書きしてもよい。

[0119] (11)本実施形態では、HDレコーダに記録されたコンテンツをSDカードにムーブする例について説明してきたが、これには限らない。HDレコーダは、ハードディスク以外の他の大容量記録媒体を備えた、DVD(Digital Versatile Disc)レコーダ、BD(Blu-ray Disc)レコーダ等であってもよいし、SDカードは、SDカード以外のICカード又はハードディスク若しくはDVDディスクその他の記録媒体であってもよい。

[0120] (12)本実施形態では、HDレコーダからSDカードへコンテンツをムーブする構成としたが、本発明はその構成に限定されるものではない。HDレコーダからコンテンツを他のHDレコーダへムーブするなど、記録再生装置から他の記録再生装置へコンテンツをムーブする構成であってもよい。

図11に示すHDレコーダ400は、HDレコーダ100に、他のHDレコーダと通信を行う送受信部311、他のHDレコーダと相互認証処理を行う認証部301、SDカード300に備えていた変換コンテンツ記憶部302、媒体記録鍵記憶部303及び部分情報記憶部304とを追加して構成されている。

[0121] HDレコーダ400と、HDレコーダ400と同構成のHDレコーダ500とを用いることにより、上述の実施形態においてはHDレコーダ100とSDカード300を用いて説明したムーブ処理、ムーブバック処理と同じ処理が実現できる。

コンテンツを記憶しているHDレコーダ400が、HDレコーダ500に対し前記コンテンツのムーブをする場合、HDレコーダ100がSDカード300に対し行っていたムーブ処理、ムーブバック処理とほぼ同じ内容の処理を行えばよいが、下記の点が異なる。

[0122] (a)上記実施形態において、HDレコーダ100は、書込読出部116を用いて、SDカード300の変換コンテンツ記憶部302、媒体記録鍵記憶部303、部分情報記憶部304に対するデータの書き込みと読み出しを行っていたが、本変形例では、HDレコ

ーダ400は、送受信部311を用い、HDレコーダ500の送受信部311を介して、HDレコーダ500の変換コンテンツ記憶部302、媒体記録鍵記憶部303、部分情報記憶部304に対しデータの書き込みと読み出しを行う。

- [0123] (b) 上記実施形態において、HDレコーダ100の認証部115と、SDカード300の認証部301の間でCPRM規格に基づく相互認証処理が行われていたが、本変形例では、HDレコーダ400の認証部310と、HDレコーダ500の認証部310の間でDTCP規格に基づく相互認証処理を行う。

また、本変形例では、HDレコーダ400及びHDレコーダ500に変換コンテンツ記憶部302、媒体記録鍵記憶部303、部分情報記憶部304を設けたが、変換コンテンツ記憶部302、媒体記録鍵記憶部303、部分情報記憶部304を設けず、変換コンテンツ、媒体記録鍵、暗号化部分ブロックを、コンテンツ記録部104に記録することとしてもよい。

- [0124] (13) 上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムであってもよい。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。ここで、コンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

- [0125] (14) 上記の各装置を構成する構成要素の一部又は全部は、1個のシステムLSI (Large Scale Integration: 大規模集積回路) から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。

- [0126] (15) 上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なICカード又は単体のモジュールから構成されているとしてもよい。前記ICカード又は

前記モジュールは、マイクロプロセッサ、ROM、RAM、などから構成されるコンピュータシステムである。前記ICカード又は前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ICカード又は前記モジュールは、その機能を達成する。このICカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

[0127] (16)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0128] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0129] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(17)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0130] 本発明は、デジタルコンテンツの記録再生を行う電気機器を取り扱う産業若しくは半導体を取り扱う産業において、電気機器として若しくは電気機器の一部として、生産、販売などがなされる。

請求の範囲

- [1] 記憶しているコンテンツを可搬型の記録媒体に移動するコンテンツ移動装置であって、
コンテンツを記憶している記憶手段と、
前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成手段と、
前記コンテンツの一部である部分データを抽出する抽出手段と、
前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換手段と、
生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込手段と
を備えることを特徴とするコンテンツ移動装置。
- [2] 前記抽出手段は、前記コンテンツの所定位置から、所定長の前記部分データを抽出する
ことを特徴とする請求項1に記載のコンテンツ移動装置。
- [3] 前記コンテンツは、少なくともフレーム内符号化された圧縮フレーム画像を含み、
前記抽出手段は、前記部分データとして、フレーム内符号化された前記圧縮フレーム画像の一部又は全部を抽出する
ことを特徴とする請求項2に記載のコンテンツ移動装置。
- [4] 前記コンテンツは、複数の固定長のブロックデータから成り、
前記抽出手段は、複数のブロックデータから1のブロックデータを抽出し、抽出したブロックデータ内にフレーム内符号化された前記圧縮フレーム画像の一部が含まれるか否かを判断し、含まれる場合に、抽出したブロックデータを前記部分データとして出力し、
前記置換手段は、前記コンテンツにおいて、抽出された前記ブロックデータに相当する部分を他のデータにより置き換える
ことを特徴とする請求項3に記載のコンテンツ移動装置。
- [5] 前記コンテンツを構成する各ブロックデータは、デジタル著作物が前記固定長毎に

暗号化されて生成されたものであり、

前記抽出手段は、

抽出した前記ブロックデータを復号して復号ブロックデータを生成する復号部と、
生成された復号ブロックデータ内にフレーム内符号化された前記圧縮フレーム画像の一部が含まれるか否かを判断し、含まれる場合に、抽出されたブロックデータを前記部分データとして出力する判断部とを含み、

前記置換手段は、前記コンテンツにおいて、フレーム内符号化された前記圧縮フレーム画像の一部が含まれると判断された前記復号ブロックデータに相当する部分を他のデータにより置き換える

ことを特徴とする請求項4に記載のコンテンツ移動装置。

- [6] 前記書込手段は、さらに、前記部分データの前記記録媒体への書き込みに代えて、前記記録媒体の媒体鍵を用いて、フレーム内符号化された前記圧縮フレーム画像の一部が含まれると判断された前記復号ブロックデータを暗号化し、前記暗号化した復号ブロックデータを前記記録媒体に書き込む

ことを特徴とする請求項5に記載のコンテンツ移動装置。

- [7] 前記書込手段は、
前記媒体鍵を保持している鍵保持部と、
前記媒体鍵を用いて、前記復号ブロックデータを暗号化する暗号化部と、
前記暗号化された復号ブロックデータと、前記媒体鍵とを前記記録媒体に書き込む書込部と、

前記鍵保持部に保持されている媒体鍵を消去する鍵消去部と

を含むことを特徴とする請求項6に記載のコンテンツ移動装置。

- [8] 前記抽出手段は、さらに、抽出した前記部分データの前記コンテンツにおける位置を出力し、

前記書込手段は、さらに、前記部分データの位置を前記記録媒体に書き込む
ことを特徴とする請求項1に記載のコンテンツ移動装置。

- [9] 前記記録媒体に記録されている変換コンテンツを当該コンテンツ移動装置に移動する前記コンテンツ移動装置において、

前記記録媒体は、前記変換コンテンツと前記部分データとを記録しており、
前記記憶手段に記憶されている前記コンテンツにおいて、前記部分データに相当する部分は、他のデータにより置き換えられており、
前記コンテンツ移動装置は、さらに、
前記変換コンテンツ及び前記部分データが記録されている前記記録媒体から、前記部分データを読み出す読出手段と、
前記記憶手段に記憶されている前記コンテンツにおいて、前記他のデータにより置き換えられた部分を、読み出された前記部分データにより置き換える再置換手段と、
前記記録媒体から、前記部分データと前記変換コンテンツとを消去する消去手段とを備えることを特徴とする請求項1に記載のコンテンツ移動装置。

- [10] 前記記憶手段に記憶されている前記コンテンツの所定位置から所定長の部分が、他のデータにより置き換えられており、
前記再置換手段は、前記コンテンツの所定位置から所定長の部分を、読み出された前記部分データにより置き換える
ことを特徴とする請求項9に記載のコンテンツ移動装置。
- [11] 前記コンテンツは、複数の固定長のブロックデータから成り、
前記記憶手段に記憶されている前記コンテンツの所定位置から所定長の部分に相当するブロックデータが、他のデータにより置き換えられており、
前記部分データは、前記複数のブロックデータのうち1のブロックデータであり、
前記再置換手段は、前記コンテンツにおいて置き換えられたブロックデータを、読み出された前記部分データにより置き換える
ことを特徴とする請求項10に記載のコンテンツ移動装置。

- [12] 前記コンテンツを構成する各ブロックデータは、デジタル著作物が前記固定長毎に暗号化されて生成されたものであり、
前記記録媒体には、抽出された前記部分データを復号し、前記復号された部分データを前記記録媒体の媒体鍵を用いて暗号化した再暗号化データが記録されており、
前記読出手段は、前記記録媒体から、前記部分データを読み出すのに代えて、前

記再暗号化データを読み出し、

前記再置換手段は、

前記コンテンツのうち置き換えられたブロックデータを、読み出された前記部分データにより置き換えるのに代えて、

前記再暗号化データを前記媒体鍵を用いて復号し、

復号された前記再暗号化データに対し、前記デジタル著作物に施されたのと同じ暗号化を施して前記部分データを生成し、

前記コンテンツにおいて置き換えられたブロックデータを、前記生成された部分データで置き換える

ことを特徴とする請求項11に記載のコンテンツ移動装置。

[13] 前記記録媒体には、前記媒体鍵が記憶されており、

前記再置換手段は、

前記記録媒体から、前記媒体鍵を読み出す鍵読出部と、

前記再暗号化データを前記媒体鍵を用いて復号する復号部と、

復号された前記再暗号化データに対し、前記デジタル著作物に施されたのと同じ暗号化を施して前記部分データを生成する暗号化部と、

前記コンテンツのうち置き換えられたブロックデータを、前記生成された部分データで置き換える置換部と、

前記記録媒体に記憶されている媒体鍵を消去する鍵消去部とを含むことを特徴とする請求項12に記載のコンテンツ移動装置。

[14] 前記記録媒体は、さらに、前記コンテンツにおける前記部分データの位置を記憶しており、

前記読出手段は、さらに、前記記録媒体から前記位置を読み出し、

前記再置換手段は、前記記憶手段に記憶されている前記コンテンツにおける前記位置のデータを、読み出された前記部分データにより置き換える

ことを特徴とする請求項9に記載のコンテンツ移動装置。

[15] コンテンツを記憶している記憶手段を備え、前記コンテンツを可搬型の記録媒体に移動するコンテンツ移動装置において用いられるコンテンツ移動方法であって、

前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成ステップと、

前記コンテンツの一部である部分データを抽出する抽出ステップと、

前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換ステップと、

生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込ステップと

を含むことを特徴とするコンテンツ移動方法。

- [16] コンテンツを記憶している記憶手段を備え、前記コンテンツを可搬型の記録媒体に移動するコンテンツ移動装置において用いられるコンピュータプログラムであって、

前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成ステップと、

前記コンテンツの一部である部分データを抽出する抽出ステップと、

前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換ステップと、

生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込ステップと

を含むことを特徴とするコンピュータプログラム。

- [17] コンピュータ読み取り可能な記録媒体であって、請求項16に記載のコンピュータプログラムを記録していることを特徴とする記録媒体。

- [18] 記録媒体であって、

コンテンツに質を下げる不可逆変換を施された変換コンテンツと、前記コンテンツから抽出された部分データとを記録している

ことを特徴とする記録媒体。

- [19] 可搬型の記録媒体と、記憶しているコンテンツを前記記録媒体に移動するコンテンツ移動装置とから成るコンテンツ移動システムであって、

前記コンテンツ移動装置は、

コンテンツを記憶している記憶手段と、

前記コンテンツに、品質を下げる不可逆変換を施して変換コンテンツを生成する生成手段と、

前記コンテンツの一部である部分データを抽出する抽出手段と、

前記コンテンツにおいて、抽出された前記部分データに相当する部分を他のデータにより置き換える置換手段と、

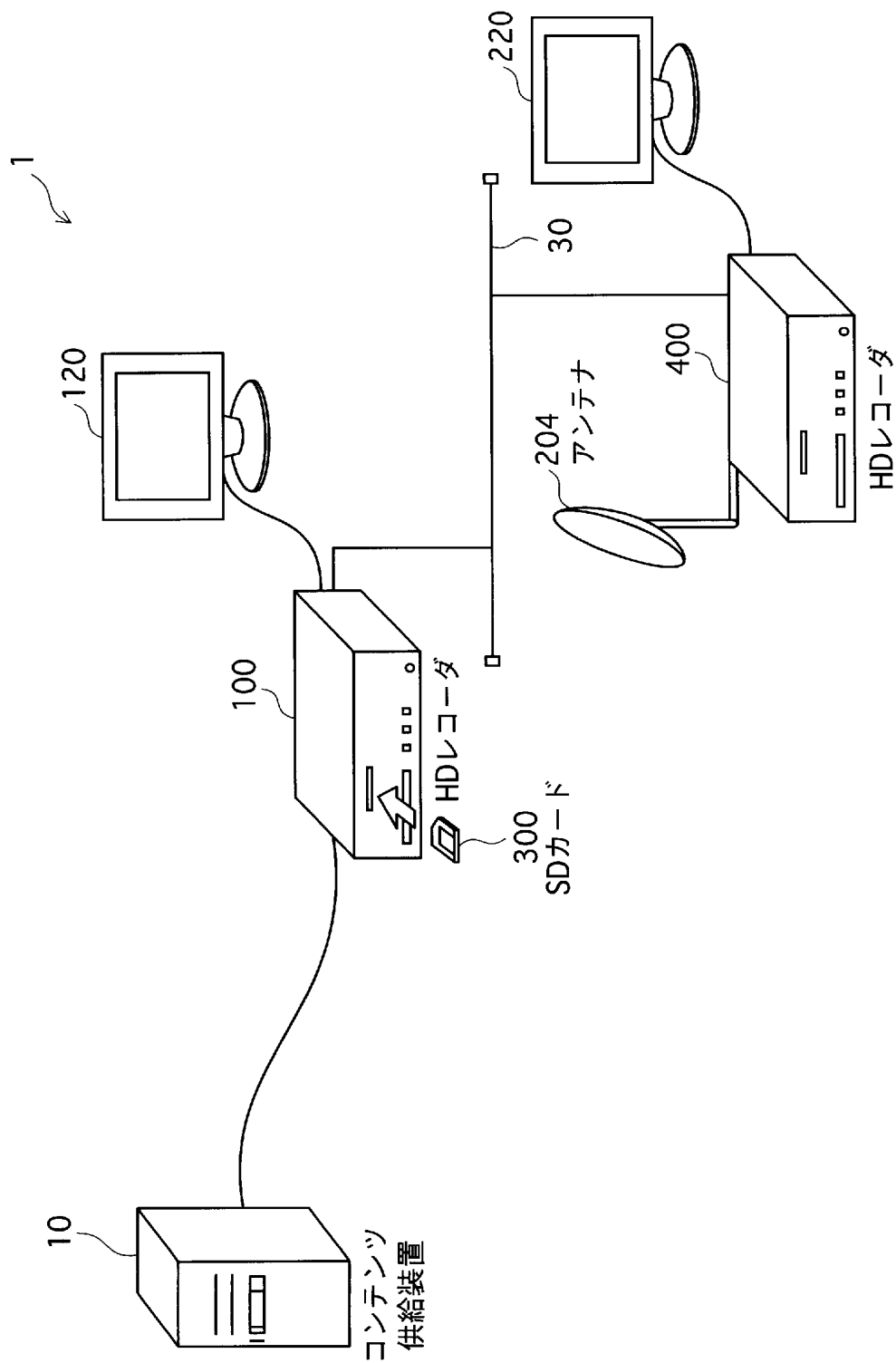
生成された前記変換コンテンツと抽出された前記部分データとを前記記録媒体に書き込む書込手段と

を含み、

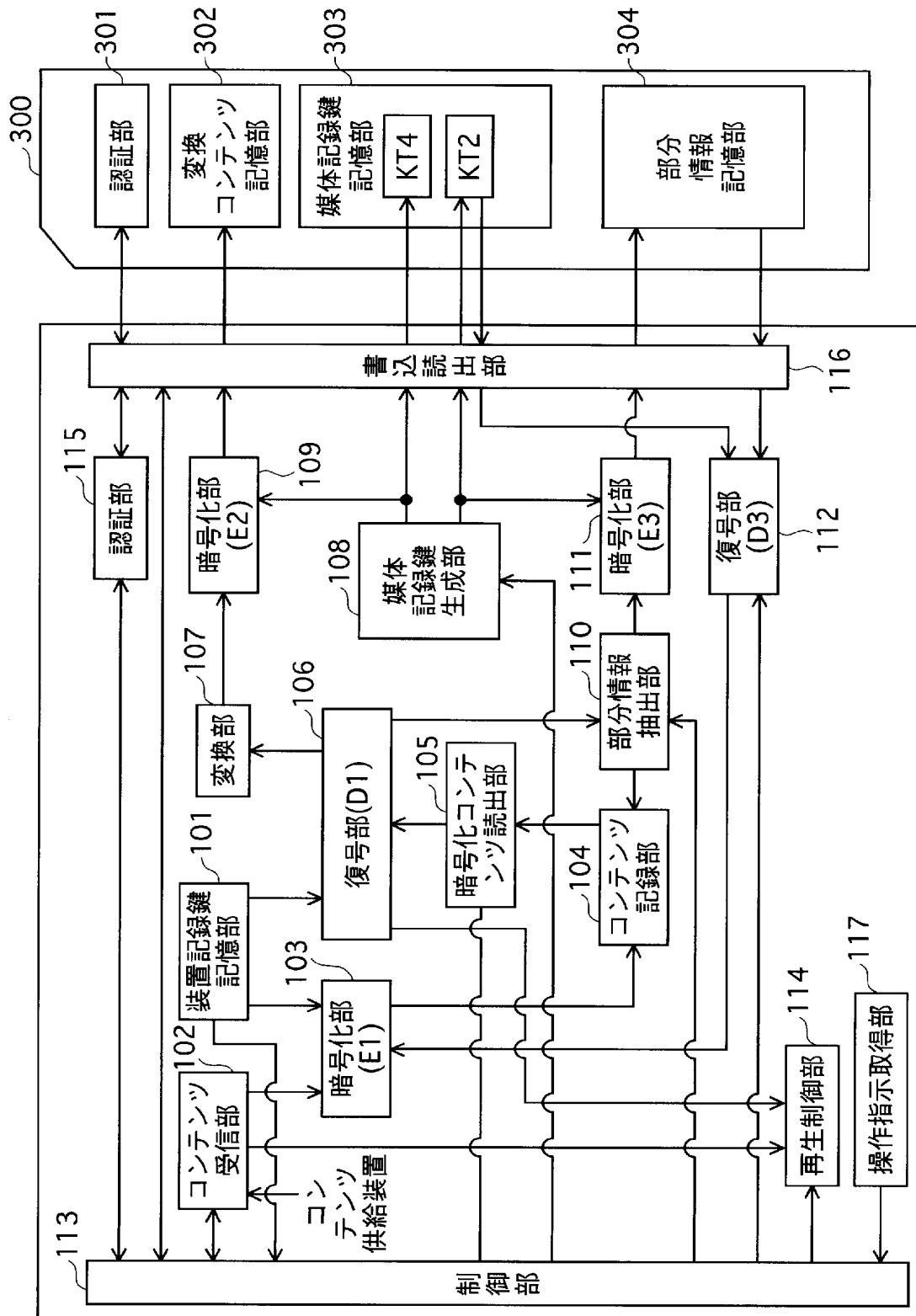
前記記録媒体は、前記変換コンテンツと前記部分データとを記録するための記憶領域を有する

ことを特徴とするコンテンツ移動システム。

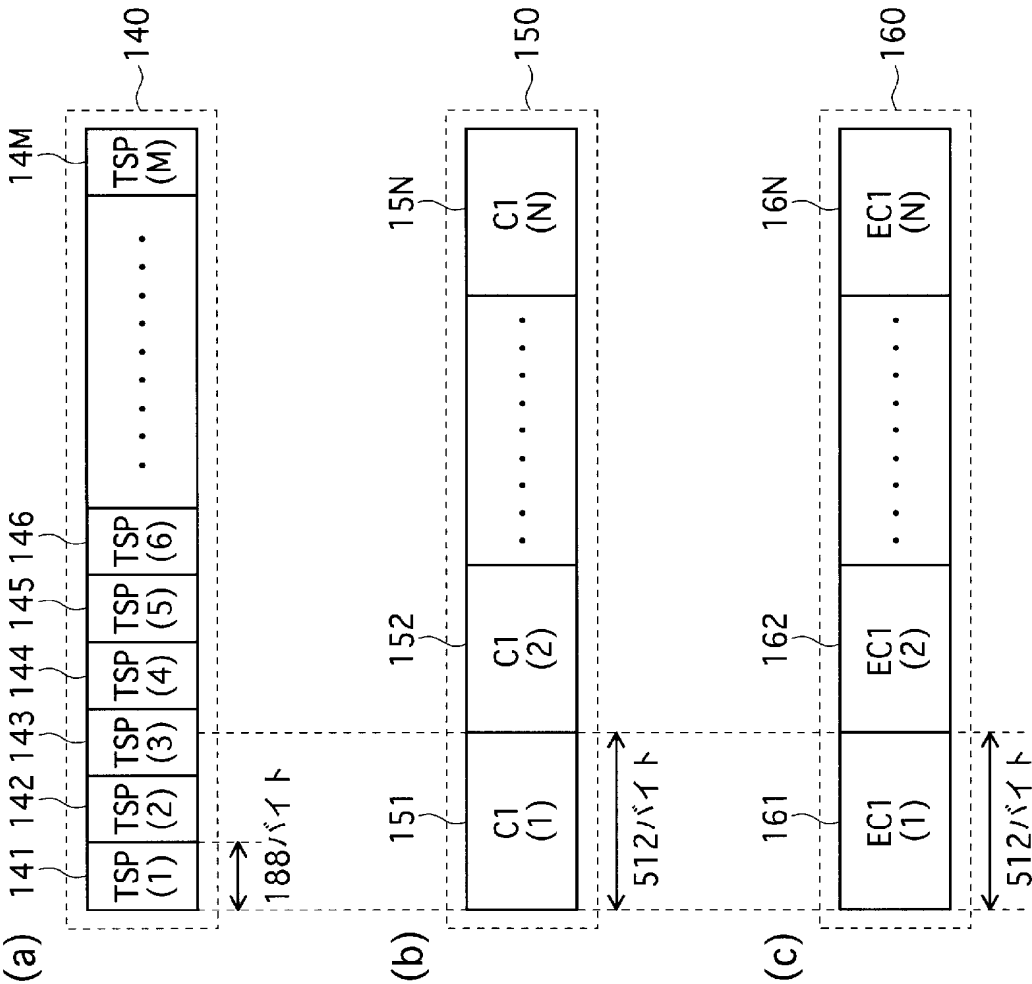
[図1]



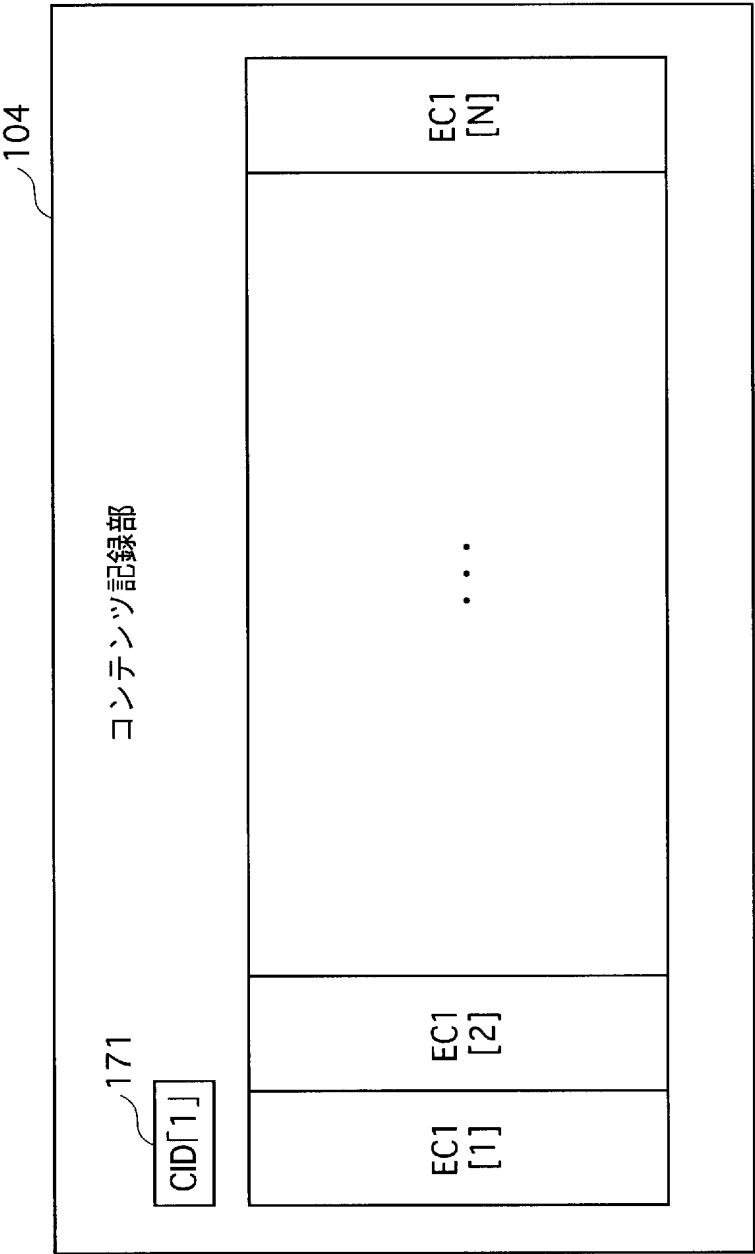
[図2]



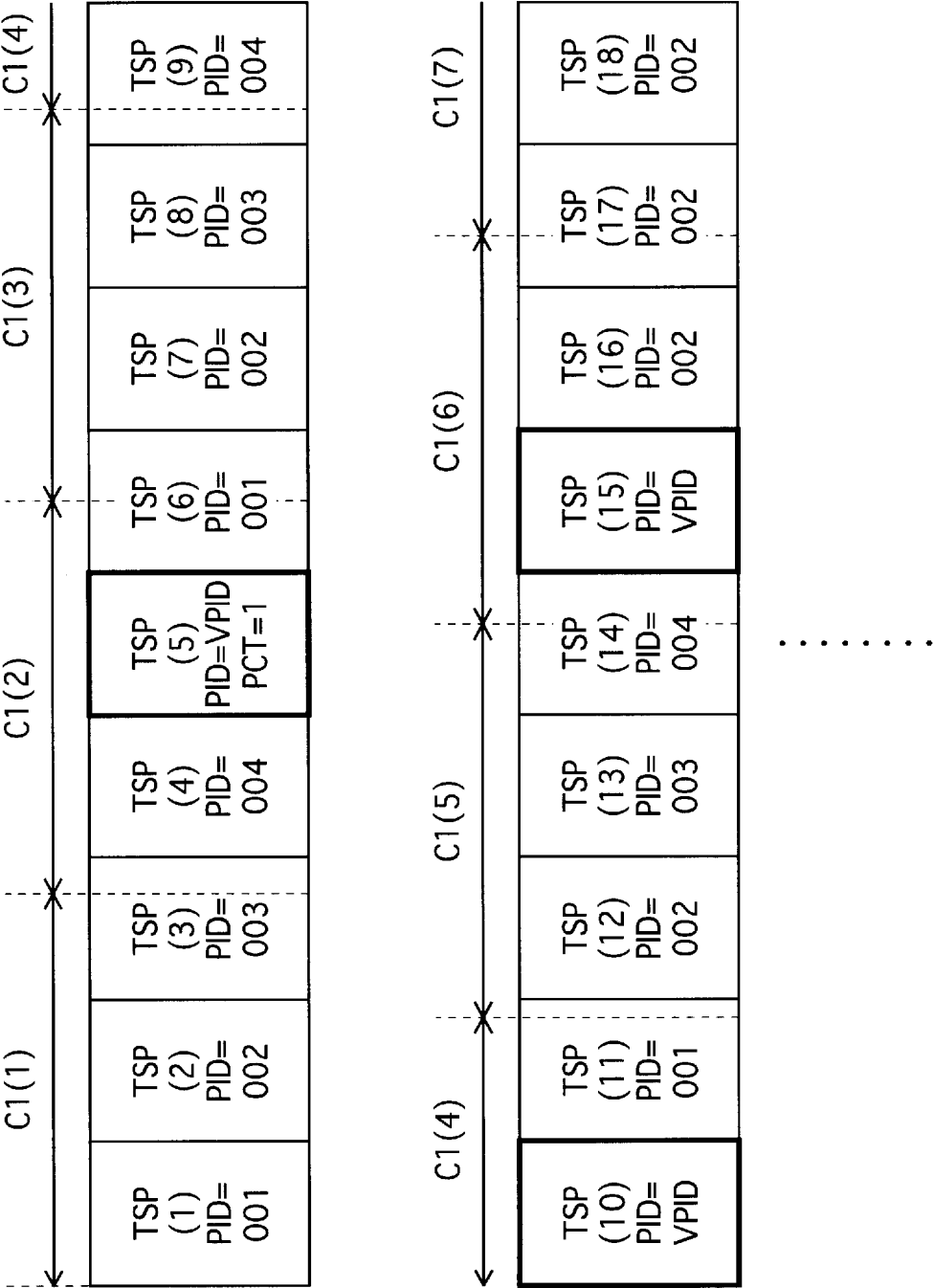
[図3]



[図4]

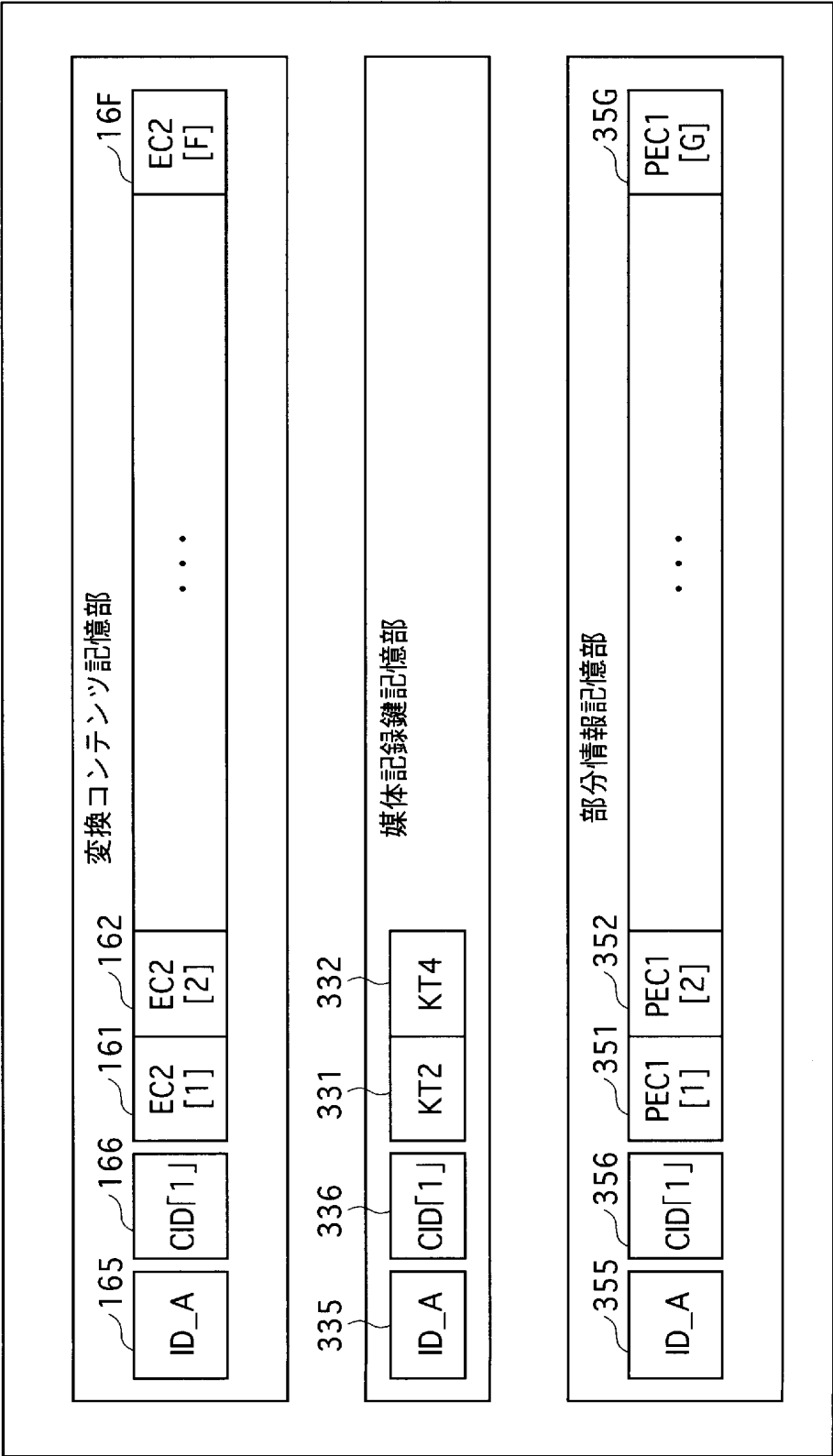


[図5]

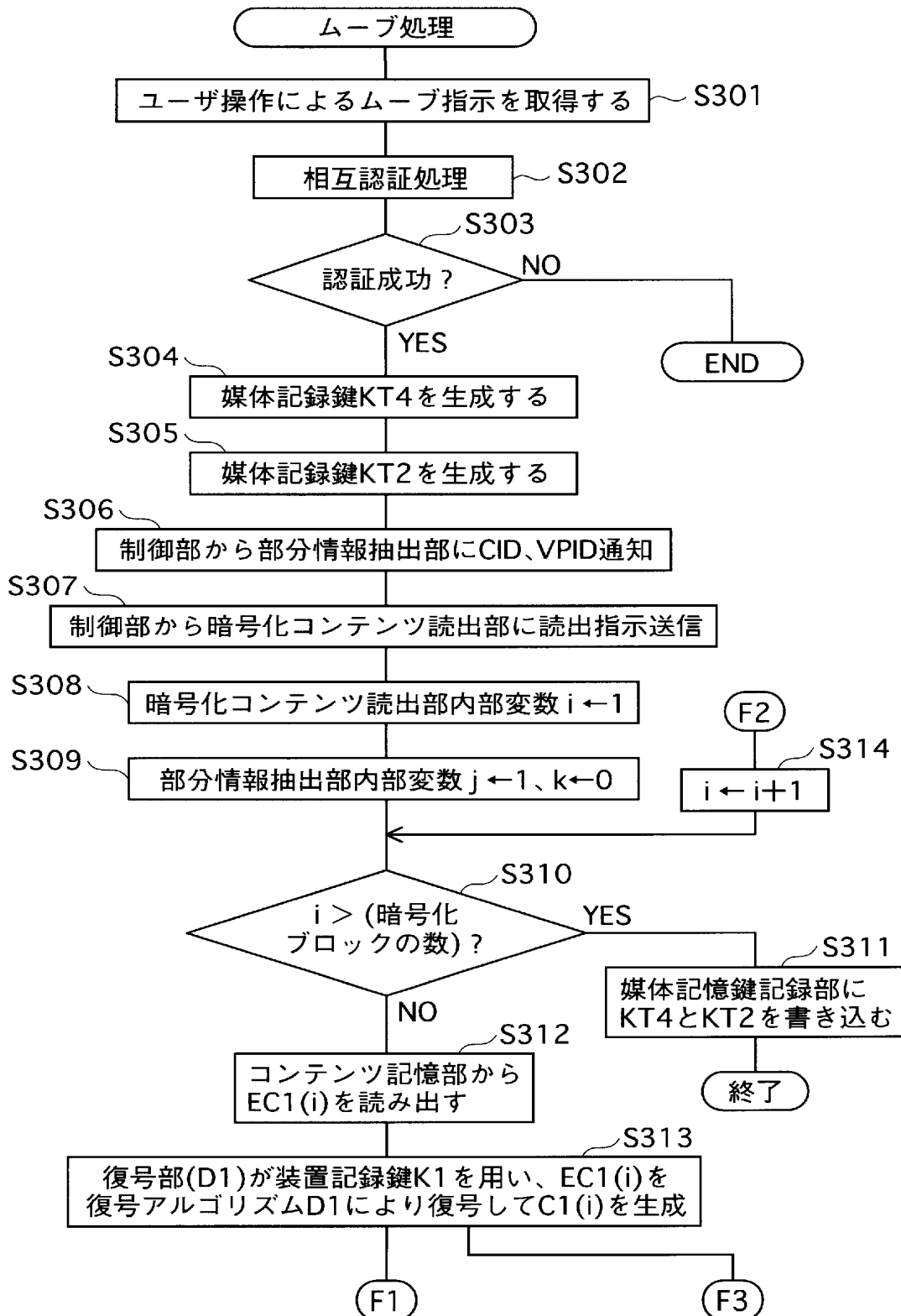


[図6]

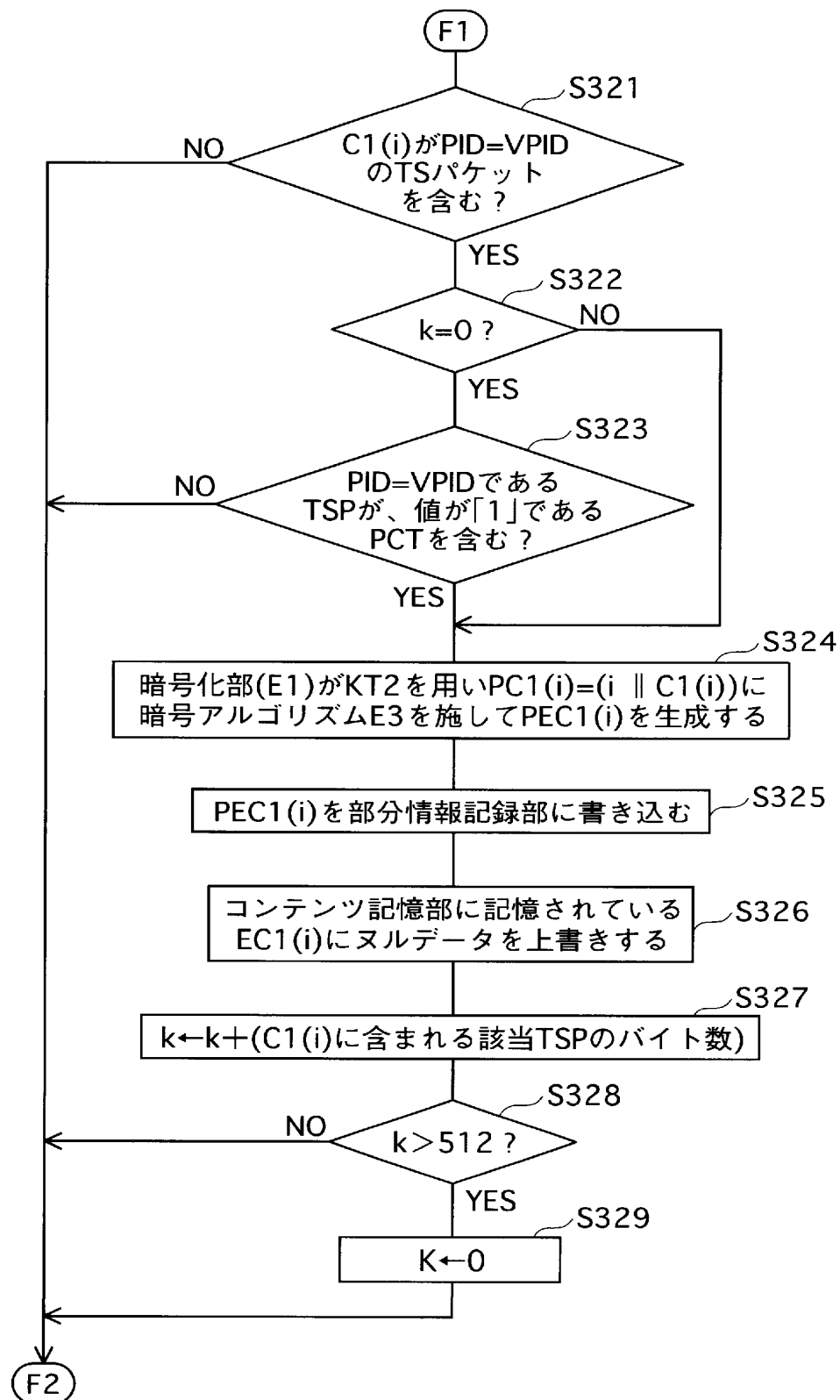
SDカード300



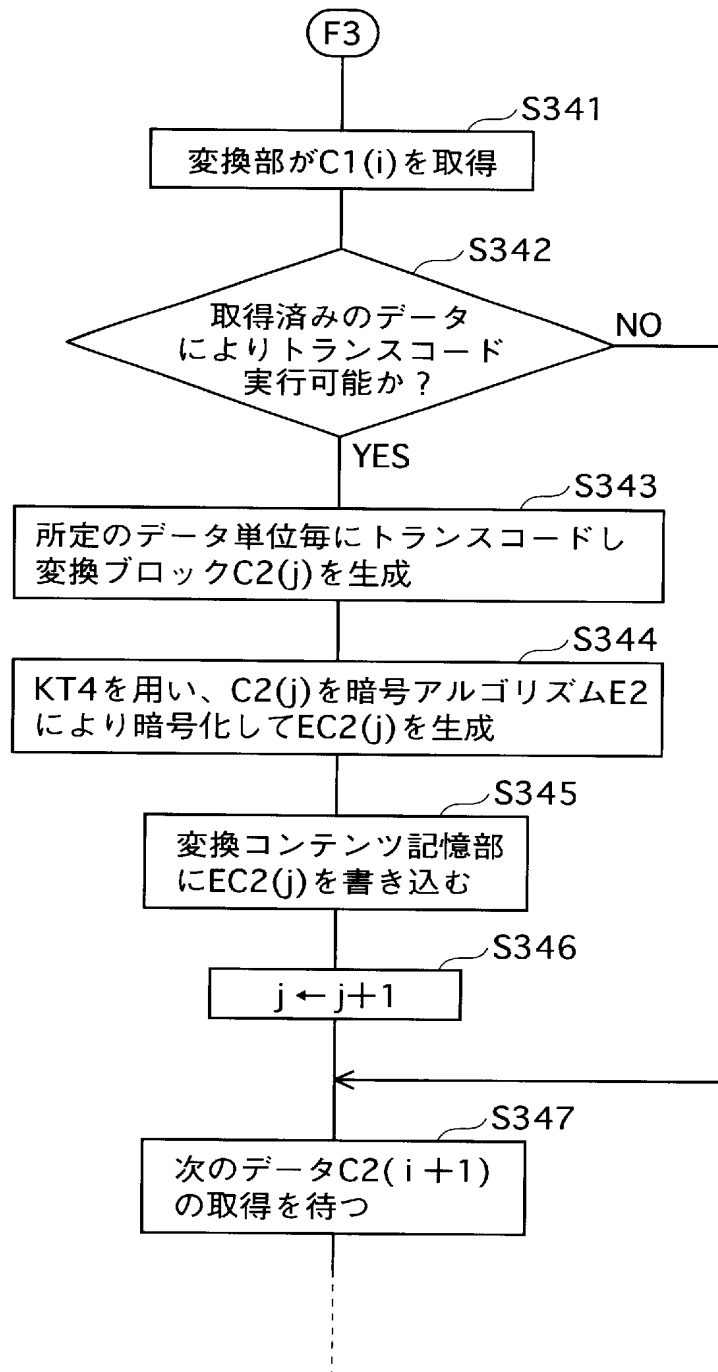
[図7]



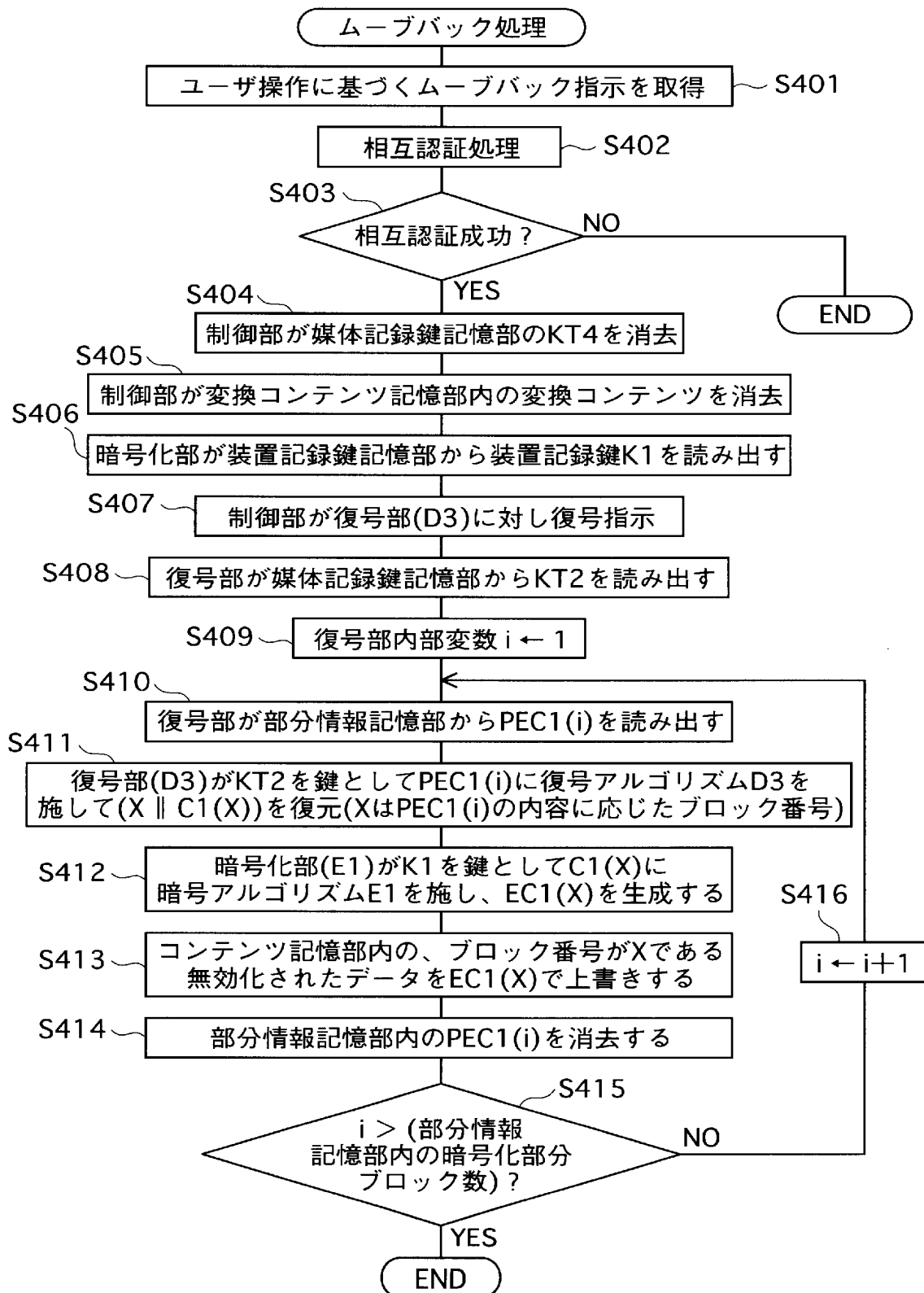
[図8]



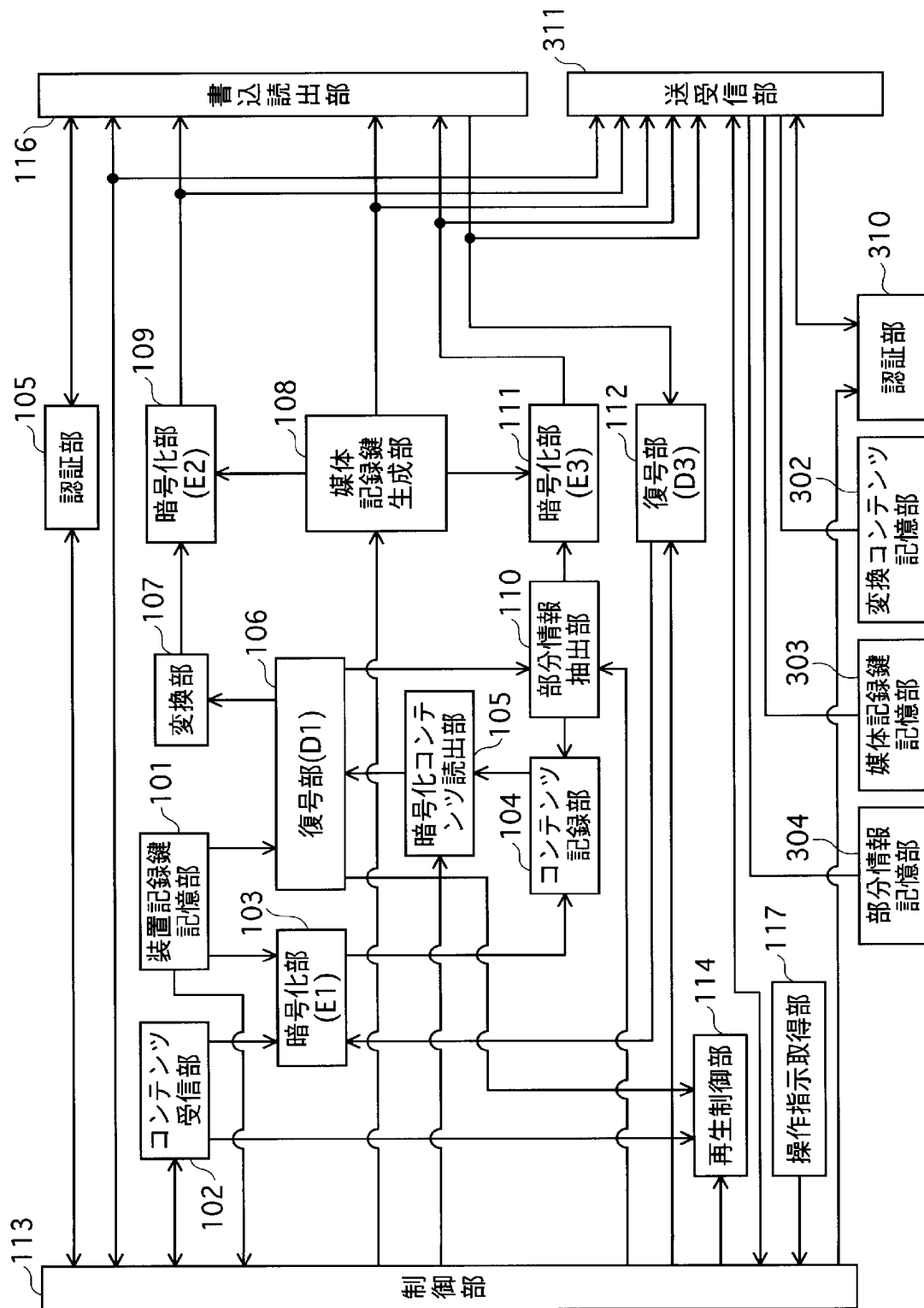
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/005253

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F12/14, G11B20/10, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F12/14, G11B20/10, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-347946 A (Deutsche Thomson Brandt GmbH.), 14 December, 2000 (14.12.00), Par. Nos. [0015] to [0017] & EP 1045388 A1 Par. Nos. [0015] to [0017]	1-19
A	JP 2004-5816 A (Toshiba Corp.), 08 January, 2004 (08.01.04), Par. Nos. [0017] to [0018] (Family: none)	1-19
A	JP 2002-278859 A (NEC Corp.), 27 September, 2002 (27.09.02), Abstract & US 2002/0143807 A1 & EP 1248433 A2	1-19

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
12 April, 2005 (12.04.05)

Date of mailing of the international search report
10 May, 2005 (10.05.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl.⁷ G06F12/14, G11B20/10, H04N5/91

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl.⁷ G06F12/14, G11B20/10, H04N5/91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 5 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 5 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 5 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-347946 A (ドイチェ トムソン・ブラント ゲーエム ベーハー) 2000. 12. 15, 段落【0015】-【0017】 & EP 1045388 A1, [0015]-[0017]	1 - 1 9
A	JP 2004-5816 A (株式会社東芝) 2004. 01. 08, 段落【0017】-【0018】 (ファミリーなし)	1 - 1 9
A	JP 2002-278859 A (日本電気株式会社) 2002. 09. 27, 【要約】 & US 2002/0143807 A1 & EP 1248433 A2	1 - 1 9

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的な技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

1 2 . 0 4 . 2 0 0 5

国際調査報告の発送日

10. 5. 2005

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区設が関三丁目4番3号

特許庁審査官 (権限のある職員)

平井 誠

5 N

9 0 7 1

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 8 6